In The Matter Of:

United States vs.

PFC Bradley E. Manning

Vol. 21

July 25, 2013

UNOFFICIAL DRAFT - 7/25/13 Afternoon Session

Provided by Freedom of the Press Foundation

VOLUME XXI

IN THE UNITED STATES ARMY

UNITED STATES
VS.
MANNING, Bradley E., PFC COURT-MARTIAL
U.S. Army, xxx-xx-9504
Headquarters and Headquarters Company,
U.S. Army Garrison,
Joint Base Myer-Henderson Hall,
Fort Myer, VA 22211
_____/

The Hearing in the above-titled matter was continued on Thursday, July 25, 2013, at 1:30 p.m., at Fort Meade, Maryland, before the Honorable Colonel Denise Lind, Judge.

DISCLAIMER

This transcript was made by a court reporter who is not the official Government reporter, was not permitted to be in the actual courtroom where the proceedings took place, but in a media room listening to and watching live audio/video feed, not permitted to make an audio backup recording for editing purposes, and not having the ability to control the proceedings in order to produce an accurate verbatim transcript.

This unedited, uncertified draft transcript may contain court reporting outlines that are not translated, notes made by the reporter for editing purposes, misspelled terms and names, word combinations that do not make sense, and missing testimony or colloquy due to being inaudible by the reporter.

APPEARANCES:

ON BEHALF OF GOVERNMENT:
MAJOR ASHDEN FEIN
CAPTAIN JOSEPH MORROW
CAPTAIN ANGEL OVERGAARD
CAPTAIN HUNTER WHYTE
CAPTAIN ALEXANDER von Elten

ON BEHALF OF ACCUSED:
DAVID COOMBS
CAPTAIN JOSHUA TOOMAN
MAJOR THOMAS HURLEY

PROCEEDINGS,

THE JUDGE: Court is called to order. Let the record reflect all parties present when the court last recessed are again present in the court.

Major Fein?

MR. FEIN: Your Honor, the next dataset CIDNE-Iraq, CIDNE Afghanistan sets. These go to Specifications 4, 5, 6 and 7 of Charge 2.

Your Honor, essentially, to use PFC Manning's own Words, the inventory of SIGACTS that he released to WikiLeaks is, quote, one of the more significant documents of our time because it reveals the true nature of the 21st century asymmetric warfare. Prosecution Exhibit 42. The document that was included the CIDNE-I and CIDNE-A SIGACTS on the SD card.

To truly understand why PFC Manning himself considered these SIGACTS so important begs the question: What is a SIGACT?

By definition, a SIGACT is a report of significant activity captured in theater. SIGACTS capture enemy activities, our responses and our TTPs to

win our wars.

For example, if the military convoy were hit by an IED, that event would be captured in a SIGACT.

Your Honor, what else would be captured in a SIGACT? Where and when the attack happened, which unit was involved, the type of IED, how successful the attack was, whether there were any casualties, which enemy organizations are responsible for the attack, what tactical intelligence we gathered from the attack and what steps we took in response to the attack. Simply put, Your Honor, SIGACTS detail how we defeat our enemies and what enemies use to harm us.

Your Honor, how do we use SIGACTS?

Mr. Hall testified that commanders in the field use SIGACTS every day to make tactical decisions.

Mr. Hall testified that intelligence analysts are often tasked to provide the commander with insights into what events have taken place along, for example, a main supply route over a certain period of time.

Intelligence analysts pull all SIGACTS taking place on that supply road. They plot those events on a map so that the commander can visualize the enemy and what the enemy is doing or not doing.

These aids help the commander understand the enemy trends and decide whether to continue using that supply route or redirect the convoy in a different direction.

Commanders use SIGACTS every day to make decisions to defeat the enemy and protect our soldiers.

As Captain Fulton testified, the commander of 210 Mountain relied on her predictive analysis and he was no different. Captain Fulton, on a weekly basis, briefed Colonel Miller on enemy trends they were identified based off of SIGACTS by PFC Manning. Those SIGACTS helped Colonel Miller decide how to employ the sources, protect soldiers.

Sergeant First Class Anica, he also gave the court an example of how the date of a SIGACT does not necessarily correlate to its value to commanders. He testified about an event that happened during a

previous deployment where two soldiers were captured by enemy forces. He explained how the unit reviewed SIGACTS for the three to four years to determine what enemy was located in that area and what tactics, techniques and procedures those in that area employed in order to figure out where those two soldiers could be found.

Those SIGACTS help the unit determine who was responsible for the captured and where they were being held captured.

Sergeant First Class Anica testified that he trained PFC Manning prior to the deployment on the use of SIGACTS and how critical they are, even older SIGACTS and how the enemy understands our forces.

Why do we store SIGACTS in SIPRNET?

SIGACTS are only available on SIPRNET because they're an invaluable resource that is released, Your Honor, to the enemy to not only teach them about our TTPs but reveal what we know about them.

Each intelligence professional from 210 Mountain testified to this point. They testified that

with this tactical insight, the enemy can adjust and become more successful in carrying out their attacks.

Why do we safeguard the tactical reports? Because those reports help us to make all the tactical decisions necessary to defeat the enemies.

The value of the tactical reports correlate to the exclusive use and benefit of this information. This is the type of information PFC Manning disclosed to WikiLeaks knowing that terrorist organizations use WikiLeaks to gather intelligence such as the marine table (inaudible).

This is not purely historical data without any value as the defense argued. Instead, this is data, this data is extremely valuable for tour commanders as part of the military decision-making process to make realtime decisions that ultimately save our lives.

Furthermore, Your Honor, the value of the tactical information to our enemies is without question -- well, is without question the value, especially given the fact that OBL himself, Osama bin

Laden himself, asked for information and received it, the SIGACTS from the CIDNE database for Afghanistan.

And now, because of PFC Manning, this is the type of tactical information that was and is in the hands of OBL on the day he died and currently in the hands of all enemies of the United States.

Your Honor, the Combined Information Data Network, CIDNE, is the direct reporting system used by all forces within the US CENTCOM.

The program manager testified that he's (inaudible) to separately track our combine operations in Iraq and also track in Afghanistan.

Your Honor, you heard testimony that a significant activity generally consists of key leader engagements, mission report logs which track troop movements (inaudible), focus on duty, status whereabouts and known DUST worm, which will you describe the names of captured or missing service members in the TTP that we employ to locate our missing service members.

Captain Lim testified that SIGACTS also

include the names of detained persons and local nationals, some of whom made these sources for neighboring U.S. source forces, (inaudible). Certain weaponry they use against the United States.

Your Honor, within seven weeks of having access to SIPRNET, PFC Manning deliberately chose to download and steal a portion of the CIDNE-I Iraq database containing more than 380,000 SIGACTS and a portion of the CIDNE-A Afghanistan database containing more than 90,000 SIGACTS.

PFC Manning had extensive experience dealing with SIGACTS at Fort Drum and FOB Hammer.

PFC Manning provided weekly briefings based on SIGACTS based off also their anticipated need because they were going to employ first Afghanistan and then Iraq.

At FOB Hammer, members of the PFC Manning unit testified that PFC Manning had constant exposure to AO, particularly the SIGACTS related to IEDs.

So what did Private First Class Manning do with these trained skills? Starting in late December

of 2009 he began exporting hundreds of thousands of SIGACTS from 2004 to 2009. That's six years or 72 months of SIGACTS from two different databases.

The CIDNE databases contained an export feature to allow intelligence analysts to export SIGACTS in 30-day increments as part of their study of enemy trends over a period of time.

Therefore, in order to export the SIGACTS, Private First Class Manning had to export them in monthly increments.

Put another way, he had to click the export classic Excel function on the bottom right of the CIDNE screen. He had to push it 72 times per database to accomplish this feat. That's a total of 144 times he had to click export to take all the SIGACTS from CIDNE-A and I databases at this time, the first part of January.

Pulling the SIGACTS from the CIDNE Afghanistan database even required more diligence and advanced understanding of the networks on SIPRNET.

PFC Manning was stationed in Iraq at the

time, deployed in Iraq.

The main CIDNE Afghanistan database was inaccessible in Afghanistan, a specific design limitation.

Mr. Holifeld testified that CENTCOM maintained CIDNE servers in Tampa as well as both theaters of operation in Iraq and Afghanistan.

The CIDNE-Iraq and Afghanistan servers do not share the same information.

The CIDNE Afghanistan database is only available to users hooked up to servers located in Afghanistan or the backup server in Tampa.

Your Honor, the defense seems to imply that PFC Manning downloaded SIGACTS to create local backup disks. In case the SIPRNET or D6-A doesn't work, the defense presented no evidence that this actually occurred. In fact, the evidence for CIDNE-A is to the contrary.

Special Agent Shaver testified that PFC Manning's computer connected with the CIDNE Afghanistan server in Tampa between 1 and 7

January 2010, the Centaur logs, again measuring net flow data captured this activity that's at Prosecution Exhibit 152, Your Honor.

The logs also show that the only times that PFC Manning's computer connected to the CIDNE-A servers in Tampa were between 1 and 7 January 2010 and no other time in the 103 days recorded in the Centaur logs.

Mr. Holifeld testified that PFC Manning pulled the last batch of SIGACTS from the SIGACT Iraq database on 3 January 2010, on 3 January 2010.

He also testified that PFC Manning pulled the batch of SIGACTS from CIDNE-A database four days later, on 7 January 2010, 7 January, 2010.

Private Manning stored the CIDNE databases in a password protected folder named yadda dot tar dot bz2 at dot NC. You heard from Special Agent Shaver, and that was on an SD card that was later found and admitted as PE92.

Special Agent Shaver also testified that this folder on the SD card was created on 30 January 2010.

He testified that he was able to view the content of this folder by using the same password PFC Manning provided Adrian Lamo on his chats.

He testified that within the yadda folder there were three different files in that encrypted file.

The portions of the CIDNE-I and CIDNE-A databases containing the SIGACTS were stored under the file names Iraq underscore events dot CSV -- excuse me, IRQ underscore events dot CSV and AFG underscore events dot CSV.

These are two CSV files which you've heard is essentially the same as an Excel spreadsheet.

Special Agent Shaver testified that the file name IRQ dot CSQ was last written on 5 January 2010 and the Afghanistan file was written three days later, 8 January 2010.

Your Honor, we knew that PFC Manning took his SD card containing more than 470,000 SIGACTS from the CIDNE-A and CIDNE-I databases with him on R and R.

Special Agent Mander testified that SD card

was found at PFC Manning's aunt's house at Potomac, Maryland where he stayed during R and R. It was during this time in R and R when PFC Manning transferred the SIGACTS from his personal computer to WikiLeaks and then his SD card onto his SD card for safekeeping.

Your Honor, the evidence shows that the transmission occurred prior to 1 February 2010 while PFC Manning was in Boston visiting friends. A transfer to WikiLeaks occurred prior to 1 February, 2010, while PFC Manning was in Boston.

How do we know this? PFC Manning forensically wiped his computer and reinstalled the operator system on 30 January 2010. Prosecution Exhibit Alpha and 126 Bravo are the install logs from PFC Manning's personal computer.

THE JUDGE: What was the Prosecution Exhibit?

MR. FEIN: Yes, ma'am, Prosecution Exhibit 126 Alpha and Bravo.

PFC Manning's aunt testified that while on R and R leave PFC Manning left Potomac, Maryland on 25

January and returned on 1 February 2010.

The disk utility log from PFC Manning's personal computer, that's Prosecution Exhibit 125, Prosecution Exhibit 125 and specifically lines 78 through 86. 78 through 86 show PFC Manning executing a 7-pass disk erase. After three hours and 48 minutes it was complete, forensically wiping his machine on 31 January 20,10, not one time, Your Honor, seven times, and after three hours it was complete.

Mr. Johnson testified that, based off his review of this log, that PFC Manning successfully wiped all of the evidence that had been deleted on his personal computer on this date. This occurred while he was still in Boston.

Your Honor, Defense Exhibit Juliet, Defense Exhibit Juliet is the forensic report for PFC Manning's personal Macintosh computer.

Prosecution Exhibit 179. Prosecution Exhibit 179 are all the attachments and enclosures to that report.

Other than the one SIGACT that Special

Agent Shaver was able to recover from March 2010 on his personal map, there are no other SIGACTS on the computer, not a single remnant of 470,000 SIGACTS from 30 January 2010 and forward -- excuse me -- 31 January 2010 on his personal computer.

The only reasonable explanation for this, Your Honor, is that PFC Manning erased any evidence of the transmission of the SIGACT to WikiLeaks when he wiped the free space on his computer on 31 January 2010.

Otherwise, some remnant of the 470,000 SIGACTS would likely be on his computer like the volume dot txt and other recovered documents. The transmission had to have occurred prior to 31 January 2010.

Once returning from Boston, PFC Manning left that SD card along with other possessions of his at his aunt's house in Maryland, and that's after disclosing the SIGACTS to WikiLeaks while he was in Boston.

Located in that same encrypted file with

the SIGACTS on the SD card, PFC Manning wrote and stored a document he called read me dot text admitted into evidence as PE42.

Your Honor, displayed on the screen is PE42. WikiLeaks, note to WikiLeaks, PFC Manning note to WikiLeaks explaining the items of historic significance, although he ignored his training and experience when it came to compromising classified information.

It is clear he applied the same training and experience to identify the SIGACTS themselves were historical significance and compilation was more of significant documents.

Your Honor, what did PFC Manning also know in late January 2010, that this information was also significant to the enemies of the United States, removing the fog of war that protected us from unconventional enemies and those that fight on the asymmetric battlefield.

Although he is the source of these SIGACTS would be protected if the information was sat on for

perhaps 90 to 100 days, he would be protected as the source if it was sat on between 90 and 180 days.

He knew, he knew that all of the intelligence and individuals named within those reports would never be protected once it was removed from the classified SIPRNET system and released to the world.

Your Honor, again that is Prosecution Exhibit 42.

Your Honor, how proud was PFC Manning of his actions knowing he was able to get away with this and finally start down the path of obtaining the worldwide notoriety.

You've seen the picture, Prosecution Exhibit 40, with the same read me dot text file. He stood smiling at his aunt's house holding the same camera that -- the SD card on the camera in this picture had 417,000 SIGACTS, the read me dot text file that he wanted to sit on the information and protect him smiling in that photo, and not protect the Iraqi and Afghanis and U.S. soldiers and everyone else in all the missions in Afghanistan.

In this particular (inaudible), Your Honor, this is not a picture of a person, of a troubled person conflicted by his action as the defense wants you to believe. This is a picture of a person who thought he was finally becoming famous with that information on the SD card.

Your Honor, the CIDNE SIGACTS were the first large scale thefts of information by PFC Manning. It is clear that PFC Manning viewed the SD card as his own trophy for his accomplishments.

Could he have kept the information erased on his personal computer and not copied over to SD card after disclosing the contents to WikiLeaks? Yes. But just like he created the mock tasking order that we would talk about later detailing his intent, PFC Manning wanted to forever memorialize for himself the fruit to his labor as he continued to exfiltrate U.S. Government databases and portions thereof.

Even five months later, Your Honor, on 26 May 2010, PFC Manning stated to Adrian Lamo that he provided what he called highlights of the disclosures

which included the SIGACTS within the CIDNE databases. That's on page 46, Your Honor, of the Lamo chats. Thus admitted to providing portions of the CIDNE-A and A database to WikiLeaks and recognizing the inherent importance of these documents.

When PFC Manning extracted records from the CIDNE database to his personal computer, he completed his theft of those records.

The SIGACTS from the CIDNE databases are stored on a classified system and only available to authorized personnel with a need to know and who could access them on SIPRNET.

At no time was PFC Manning authorized to house those records on his personal laptop or on his SD card at his aunt's house.

Furthermore, PFC Manning converted the information of the records from the CIDNE databases from, he conveyed them to WikiLeaks for publication.

PFC Manning specifically intended for the records to be released and WikiLeaks obliged. The United States devoted significant resources to protect

this classified information.

Mr. Lewis testified that foreign intelligence services will pay for the information precisely because its exclusive possession provides a significant benefit to the United States. The publication of SIGACTS from the CIDNE databases completely deprived the United States of this exclusive possession of the use of that information.

Your Honor, PFC Manning knew the charge documents for specifications 5 and 7 of charge 2 were classified. These documents are probably marked secret within the classified information field of SIGACT reports.

Further, these documents are located on SIPRNET and the United States has not made these documents available to the public. They were closely held.

The charged documents themselves for specifications 5 and 7 of charge 2 relates to the national defense of the United States. Lieutenant Commander Hoskins and Lieutenant Colonel Nehring both

testified the documents contained a type of information which would cause serious harm to national security and thus should be secret.

It was the type of information that could be useful to our adversaries and the type of information that PFC Manning knew would be useful to the adversaries.

Admiral (inaudible) US CENTCOM deputy commander and the OCA testified that the charge documents within both datasets, the CIDNE-I SIGACTS and CIDNE-A SIGACTS, are classified at secret level because their release could cause harm to national security.

Your Honor, if I may have a moment.

THE JUDGE: Yes.

MR. FEIN: Your Honor, PFC Manning and Major Hurley have relocated to the witness box in order to look at classified information and I have handed them each a copy and the Court Appellate Exhibit 617, the government classified supplemented closing argument.

Your Honor, Mr. Lewis testified that the

value of the SIGACTS from the CIDNE-A database far exceeds the statutory minimums.

Specifically, Mr. Lewis testified that the Foreign Intelligence Services of multiple countries actively seek information contained within the SIGACTS and would pay money from the SIGACTS from CIDNE Afghanistan.

The Foreign Intelligence Services seek information pertaining to the United States military tactics, techniques and procedures, TTPs, which show operation strategies, responses to attacks and the units involved in TTPs and military operations in Afghanistan detailed in classified reason number 1.

Your Honor, when you're finished looking at classified reason 1, would you please let me know and I'll continue.

THE JUDGE: I have.

MR. FEIN: Yes, ma'am.

Your Honor, Mr. Lewis testified that country 1 would pay at least $10,000 for the compromised SIGACTS from the CIDNE-A database and

Mr. Lewis called his valuation conservative as set forth in classified reason 2.

Your Honor, a Foreign Intelligence Service has paid $50 each for documents containing information similar to that found in the SIGACTS. Mr. Lewis determined that a Foreign Intelligence Service would value at least 30 percent of the SIGACTS from the CIDNE-A database.

Based on Mr. Lewis' evaluation and the price paid per document, the 90,000 SIGACTS from the CIDNE-A database are worth approximately $1.3 million to a Foreign Intelligence Service.

Your Honor, that is 30 percent of 90,000 documents times $50.

Your Honor, Mr. Lewis also testified that the value of the SIGACTS from the CIDNE-I Iraq database far exceeded the statutory minimums.

Specifically, Mr. Lewis testified that the Foreign Intelligence Services of multiple countries actively seek information contained in the SIGACTS and would pay for SIGACTS from the CIDNE-I rack database.

The Foreign Intelligence Services seek information pertaining to the United States military tactics and procedures which show operational strategies, responses to attacks and the units involved in TTPs of military operations in Iraq as detailed in classified reason number 3.

Mr. Lewis testified that country 2 would pay at least $10,000 for the records in the CIDNE-I rack, the SIGACTS in the CIDNE-I rack database, and Mr. Lewis called his valuation conservative as set forth in classified reason 4.

A Foreign Intelligence Service has paid $50 for documents containing information similar to that found in the SIGACT. Mr. Lewis determined that a Foreign Intelligence Service would value at least 10 percent of the SIGACTS from the CIDNE-I database.

Based on Mr. Lewis' evaluation, the price paid per document, the 380,000 records, SIGACTS in the CIDNE-I database are worth approximately $1.9 million to a Foreign Intelligence Service which is 10 percent of $3,850,000 times $50.

Your Honor, at this point I'm going to move on to the ACIC document which doesn't necessarily -- doesn't require any classified enclosures to be referenced.

THE JUDGE: Do you request to retrieve them and have PFC Manning go back to the table?

MR. FEIN: Yes, ma'am, I do. So the United States requests that I will collect those documents and continue.

Your Honor, United States retrieved Appellate Exhibit 617 from the court and PFC Manning and Major Hurley.

Your Honor, the next document, compromised document is the ACIC document and this goes to specification 1 -- excuse me, Your Honor -- 1 and 15 mostly for (inaudible) offense, Your Honor, specification 15 Charge 2.

Your Honor, the ACIC report is a charge document. The declassified version of the document is at Prosecution Exhibit 45 and the original classified version is at Prosecution Exhibit 46, 45 and 46.

Your Honor, the ACIC report provided PFC Manning with the actual knowledge that the enemies of the United States would use classified information obtained from WikiLeaks against the United States and knowing that PFC Manning deliberately disclosed this document, this document to the world through WikiLeaks.

Ms. Gwynn testified about the Army Counterintelligence Center's process for creating intelligence products like self-initiated special report charged tier. She also addressed the center's meticulous sources program.

With regard to the report significance, she explained the mission of the cyber counterintelligence assessments branch where he worked as a senior analyst was to identify the specific threats using predictive analysis and use work product like the charge ACIC document that she explained reflects that objective.

Your Honor, in this case the 18 March 2008 report describes in detail what the other research of WikiLeaks.org revealed about the nature, operations and actions of WikiLeaks in 2008. Its purpose was to

assess the counterintelligence threat posed to the United States Army by the WikiLeaks website.

Specifically, the ACIC report analyzes the threat posed by WikiLeaks following the release of the U.S. Army table of equipment in Iraq and Afghanistan from April 2007 and the release of other classified U.S. government information.

The report's key judgments communicate three main points, Your Honor. That WikiLeaks represents potential force protection counterintelligence OPSEC and INFOSEC threat to U.S. Army, pages 3 and 4 Prosecution Exhibit 45.

Recent unauthorized releases of DoD sensitive and classified information provide Foreign Intelligence Services, foreign terrorist groups and other adversaries with potential actionable information for targeting U.S. forces.

And WikiLeaks most likely has other DoD sensitive classified information in its possession and will continue to post it on their website.

Your Honor, the ACIC report goes on to

discuss DoD classified information that WikiLeaks had released in the past and how WikiLeaks posts all information that it received without editorial oversight.

The basic report concludes that and PFC Manning knew that it must also be presumed that foreign adversaries will review and assess any DoD sensitive or classified information posted to that website.

The document warned readers of adversaries' increased ability to complete rapid data compilations to more efficiently develop actionable information, intelligence collection, planning or targeting purposes against the United States.

That's on page 21, Your Honor, of Prosecution Exhibit 45.

So you'll see, Your Honor, that this charge document serves as another warning to PFC Manning as to the dangers of posting information on the internet generally and once more on WikiLeaks specifically.

Given the accused's experience with the

classified information of classified documents and the types of information contained in that report as well as its markings, the accused knew that the unauthorized release of that single report itself could cause serious damage to national security.

As you heard from Ms. Gwynn, the ACIC document is only available on SIPRNET. At the time it was taken from the U.S. Government or on (inaudible) and transmitted to WikiLeaks and ultimately posted to the internet.

The report was marked secret at the top and bottom of each of the 32 pages which (inaudible) to PFC Manning that it was a classified information and should be treated as such.

Your Honor, Prosecution Exhibit 181 Alpha, 181 Alpha is the classified stipulation expected testimony for the original classification authority of that document and it further explains why the ACIC report is national defense information and was properly classified at the secret level. Prosecution Exhibit 181 Alpha.

Your Honor, Prosecution Exhibit 84 is a summary of the Intelink logs produced by Special Agent Shaver to annotate the exact time PFC Manning downloaded this document and viewed the ACIC document for Intel.

This shows PFC Manning accessed the web page that contained the document dot ASP version and the document version, that's the Microsoft Office document, the DOC version of the ACIC report on 29 December 2009, 14 February 2010, 1 March 2010, and all that from his dot 40 SIPRNET computer.

Your Honor, Mr. Arteli, the ACIC website administrator, he testified that Prosecution Exhibit 63, an IP address associated with PFC Manning accessed the ACIC website containing the ACIC report on 1 December 2009 and subsequently on 29 December, 1 March and 7 March.

Mr. Chamberlain testified that the IP address addresses dot 22 and dot 40 accessed ACIC server 114 times beginning on 19 November 2009 and that is reflected in the server logs, Prosecution Exhibit

64.

THE JUDGE: How many times did you say?

MR. FEIN: Your Honor, 114 times beginning on 19 November 2009 which is essentially within a few days of PFC Manning having access to SIPRNET without a soldier to his left or right during RIP/TOA.

Your Honor, the first time the United States can prove PFC Manning viewed the ACIC report was on 1 December although he accessed the website on 19 November. PFC Manning was on the ACIC website viewing that document weeks before Christmas Eve of 2009.

Your Honor, what did PFC Manning do after reading the ACIC document, ignoring the warnings enumerated in the document and then compromise the ACIC document to WikiLeaks. He obsessively followed its release and (inaudible) in the amount of press the release was receiving.

And in the Assange chat PFC Manning makes clear his need to monitor the attention his actions were receiving.

PFC Manning told Julian Assange that a US

Government official, Lieutenant Colonel Packnett, confirmed the authenticity of the ACIC reports to the New York Times laughing this action is contravention of the typical policy to protect classified information by neither confirming or denying the authenticity of classified information.

Your Honor, that's clearly stated in the Assange chats page 13.

Your Honor, the accused repeatedly searched cables on WikiLeaks. He repeatedly accessed it and ultimately disclosed it to WikiLeaks. The intelligence report relates to national defense discussing specifically our vulnerabilities to WikiLeaks and the terrorist organizations their actions aid.

This document was classified and not released publicly until PFC Manning took it upon himself to unilaterally decide the world, including the enemies of this country, should receive it.

Your Honor, the next charged document is the Apache video. This is specification 2 of charge 2.

Though edited by WikiLeaks and PFC Manning

for release, the video is compromised by PFC Manning with over 38 minutes of footage from United States to the Apache helicopter.

Ultimately, the WikiLeaks was posted to the world on 5-8-2010, to the activist organization on 15 February 2010.

With regard to the content of the video, Your Honor, you heard primarily from Chief Warrant Officer 5 John LaRue has been an Apache helicopter pilot more than quarter of a century flying Apache helicopters. (Inaudible) depicts the display of the Apache helicopter.

He shows the angles of depicts how pilots use technology on aircraft and exposes our use of laser technology to obtain key metrics.

Overall, the video documents the actions and experiences of U.S. service members conducting a wartime mission.

With regard to the manner in which the video is treated, Chief LaRue testified that the footage contains a sort of information preserved to

facilitate lessons learned by our aviation community and that protected from compromise by placement on SIPRNET system.

The information is reviewed and sanitized prior to any potential public release. Although the Apache video is classified, it's sensitive.

The senior pilot testified that this information is the same type he had been taught and himself teaches never to release.

Why is that, Your Honor?

As Chief LaRue explained, this information benefits our adversaries by communicating our tactics, techniques and procedures and informing them on the limitations of the U.S. government's technology.

Your Honor, the defense would have you believe that a verbatim transcript of the incident had already been made public and this somehow showed the video wasn't closely held and excuses the accused's conduct. This United States myth is actually a red herring.

Just as purported state cables contain

topics also addressed in open source material, so is true the incident depicted in the charged video was no secret.

However, just like every other piece of protected U.S. government material in this case, at no point was the entirety of this video officially released and no point were images made public and no point was the TTP information contained disclosed. Even the book itself didn't describe the weapons or engagement response.

Moreover, the transcript in the Finkel book is not actually verbatim although the portions are similar. There's been no evidence that the embedded journalist ever saw the video, and the author mentions the sensitivity of protecting the sources and methods from which the content is derived, the content of his book.

What's more is that based especially AIT and on-the-job training already discussed, PFC Manning knew the value of the video to the enemy as well as the need to protect the information it contained.

Disregarding the sensitivity of this material, PFC Manning thought the video was cool and decided to release it to a bunch of anti-government activists and anarchists to achieve a maximum exposure, the maximum exposure and advance his personal quest for notoriety.

Ultimately, this video is released by WikiLeaks, yet PFC Manning's involvement in this tale and the compromised region as far back the December of the previous year. PFC Manning saw, researched, released and then assisted in doctoring the video for maximum impact, all notwithstanding his understanding of the nature of the material.

PFC Manning first saw the video in December of 2009 with soldiers in unit. Ms. Showman, Captain Fulton, Chief Balonek all testified that the video was located on the unit SIPRNET, their SIPRNET share drive.

This drive Captain Cherepko testified was acceptable to any individuals with appropriate clearance such as PFC Manning and his analyst colleagues.

Your Honor, 22 January 2010, 22 January 2010, PFC Manning left Iraq for his R and R leave. During this time he erased his computer in order to destroy any evidence regarding the Gharani video and the CIDNE databases, the SIGACTS portions of the CIDNE databases.

By this point, Your Honor, in 22 January 2010, PFC Manning realized that his previous Gharani leak would not be released any time soon because it was encrypted. This reality was essentially utterly unsatisfactory to them.

Through researching the event, PFC Manning released the Apache incident had been subject to a FOIA quest. This Apache video was his opportunity to and therefore would be his next target.

PFC Manning, returning to theater on 14 February 2010, less than 24 hours later on 15 February 2010 he burned the Apache footage and its associated documents onto a disk from his SIPRNET D6-A computer and he took that material out of the T-SCIF to his shoe where he loaded into his personal McNamara

computer uploaded 20 WikiLeaks.

That video, along with the Reykjavik 13 learn cable and (inaudible), Your Honor, this is shown by the forensic evidence.

Prosecution Exhibit 127 is the volume dot TXT document line 1, line 1 on PE127 shows the Apache file name which was the same name he used for the file in the disk found in his shoe at the time of his arrest.

However, Your Honor, compromising Apache video to WikiLeaks wasn't going to be enough for PFC Manning. The entire video would not make the splash he wanted and garner the attention he craved.

PFC Manning didn't get the reaction he desperately wanted from that Gharani video. It couldn't be released because WikiLeaks didn't have the password. This meant that PFC Manning was deprived the notoriety his actions deserved.

If WikiLeaks didn't make the press, how could he be the one that hailed the source. PFC Manning wanted to make sure this video, this video

that the day after he got back from R and R made the biggest splash and it received the most attention.

So accordingly, Your Honor, PFC Manning ultimately participated in editing the video which would later be released by WikiLeaks under the name of "Collateral Murder."

Your Honor, this is Prosecution Exhibit 41. Page 1 an e-mail between PFC Manning and Mr. Schmidle.

Note, please, Your Honor, that PFC Manning credits himself in this e-mail with, quote, approving the edits and instructing the quotation inclusion.

Paragraph one of his own e-mail. I approve the edits without actually viewing the video, had a written description.

Then he talks about instructing the, well, quote, paragraph 3. You should note too, Your Honor, the hypocrisy for professing all the information needed to be public, PFC Manning did not seek to release the whole video but rather an edited version to maximize impact.

And instead of leading the people he wanted

so much to have the information, free to assess it. There should be no transmitted. The only thing --

(Whereupon, there were announcements in the media room interrupting audio.)

MR. FEIN: Your Honor, these are not the actions of a naive person stumbling onto something he thought should be made public. Instead, this a capable soldier being trained with his experience regarding the enemy's priorities and resources and with an agenda, Your Honor, he's a soldier that can't live on his skills, training and access for his own personal gain. He put himself before his country even with this video, Your Honor.

Virtually each click of his mouse on SIPRNET was motivated by his request for the biggest impact and the widest notoriety. With the editing of the Apache helicopter video, he knew he would get a reaction. Over and over he conducted open source, he (inaudible).

First, Your Honor, PFC Manning conducted searches for Reuters, Apache helicopter video related

items 51 times, 51 times in 36 days between March and April of 2010. This is all in the Intel link search summary, Prosecution Exhibit 81, lines 534 through 668, 534 through 668.

THE JUDGE: That's Prosecution what?

MR. FEIN: 81, Your Honor, Intelink search logs.

PFC Manning used search to search open source articles on the SIPRNET system 61 times. He also edited the collateral one murder video on his dot source computer.

In an effort to obtain immediate notoriety, although in a clandestined form PFC Manning brought to the attention of Captain Fulton who compared the link share drive video to verify a match noting her reaction, he burned the souvenir copy three days later.

Then in May PFC Manning discussed via e-mail his role in editing that video as you saw a moment ago to Mr. Schmidle saying he was glad it made an impact in connecting it to the CIDNE actual reports of the SIGACTS.

Finally, PFC Manning's own aunt testified that PFC Manning asked her to post the edited version on his Facebook account after being confined.

The theme here is PFC Manning's consistent cavalier attitude towards this material. Manning knew the importance of the information and that it was only available on SIPRNET.

He even thought it was classified. So based on his knowledge, training and experience, he knew it was not publicly available.

Ms. Scott, the chief of FOIA and privacy section for U.S. CENTCOM, she testified while the investigation has been released to the public through FOIA, this specific video was not released.

At every turn, Your Honor, PFC Manning's handling and treatment of this video has been a violation of the United States.

PFC Manning copied what later determined to be an unclassified video, took to his room for unclassified use to (inaudible) what he thought was an intelligence (inaudible).

Your Honor, he took these deliberate steps even when the book he talked about in these chats, self claimed measuring stick for this disclosure revealed the author had not released the entire video transcript and did not release any images from the video itself, and it deliberately protected sources and methods within his own book, page 285, and Prosecution Exhibit 186.

Your Honor, the next section, password cracking, specification 1 charge 3. You've heard --

THE JUDGE: What?

MR. FEIN: I'm sorry. Specification 1, Your Honor, of charge 3.

THE JUDGE: Okay.

MR. FEIN: Your Honor, you've heard overwhelming evidence that PFC Manning started using his access to SIPRNET less than two weeks after starting work in the SCIF at FOB Hammer.

By March 2010, the accused stole and transmitted over 20,000 documents and watched the world's reaction to the cables released.

One of the topics the United States did not highlight were some of the things PFC Manning conducted on SIPRNET related to obfuscating his internet activity.

Between 6 December '09 and 8 March 2010, PFC Manning searched 19 times on SIPRNET for terms such as encryption, and that's what PFC Manning described to Ms. McNamara as encryption that has gone 12 years not being broken in his chats. And MD5, which is an algorithm for hashing files.

Then, on 8 March 2010 at 22:28, so 10:28 p.m., PFC Manning used his access to SIPRNET to search for rainbow tables --

THE JUDGE: What date was that?

MR. FEIN: Ma'am, that's on 8 March 2010, at 22:28:21 seconds. More importantly, Your Honor, it's line 417 of Prosecution Exhibit 81. Line 417 Prosecution Exhibit 81.

That search was for rainbow tables. Why would PFC Manning be doing research on rainbow tables. It's pretty obvious when you put the pieces together

and gets to the heart of Specification 1 of charge 3.

We know that PFC Manning was obsessed with covering his own tracks. We know this from his personal Mac information erasure on 31 January 2010. He performed a 7-pass erase of his computer, not just one. These facts join a host of others which evidence PFC Manning's interest in hiding his transgressions.

He used other people's user accounts and he changed the default setting on his dot 22 internet browser to refrain from capturing internet search history.

But at some point, Your Honor, at some point, it occurred to PFC Manning that there might be a chance that his activity was being captured by audit systems on the SIPRNET.

It was easier to obfuscate what he was doing on his own machine, but not as easy on the SIPRNET. And, in fact, we know that it was a concern of his from his chats with Julian Assange.

Your Honor, on page 3, Prosecution Exhibit 123, Assange chats, PFC Manning said ha, I'm all over

the place, clearing logs, not logging at all, safe, I just wanted to be certain. And this was on 6 March 2010, talking about clearing logs. So, again, why search on Intel link for something called rainbow tables on 8 March 2010.

PFC Manning SIPRNET computers had a local user named FTP user on the account. You heard from Special Agent Shaver that the FTP user, the user name was a user account on the D6-A SIPRNET computers and was not attributable to any particular person or user.

It was an account that would store files without any tie to the actual user behind the keyboard.

It was an account where one could store programs like Wget within the profile my documents and not have any tie to the ultimate user behind the keyboard. It's an account one could search the SIPRNET and get closely held information without any tie to the actual user behind the keyboard.

In short, Your Honor, having access to the FTP user account could effectively anonymize PFC Manning behind the keys of the dot 22 and dot 40

SIPRNET computers.

Fortunately for the United States, the PFC Manning's attempts to gain access to the FPT user account would fail despite from the assistance from Julian Assange and WikiLeaks.

Special Agent Shaver testified that Microsoft Windows has multiple ways to protect passwords.

First, instead of storing the actual password in plain text, the actual words of the password, the letters and numbers, Windows converts it to a unique hash value and that's called the LM hash. LM hash. And it uses a complicated mathematical algorithm to prevent what Special Agent Shaver called bad people from obtaining passwords.

Second, Your Honor, Windows, Microsoft Windows splits that algorithm into two pieces, storing one in the computer's system file and one in the computer's SAM file, system file and SAM file.

Finally, Windows, the last layer of protection that Windows provides is that it locks down

these two files, the system file and SAM file. It locks them down so no user except an administrator can actually access the content of those files.

Your Honor, no, he did not have administrative privileges. PFC Manning resorted to the most effective method of circumventing the sort system on his SIPRNET computer. He decided to bypass all of Microsoft Windows, the entire operating system of Windows to access the security information on the computer.

He did that knowing the protection Microsoft Windows has on the SAM and system files.

Special Agent Shaver testified that if the user was to boot their computer using a CD that was configured to run another operating system, that user could navigate to the SAM file or system file on the hard drive and view its contents because that's doing it outside of Windows.

One such operating system is Linux. Special Agent Shaver testified that a knowledgeable person could download a copy of Linux free from the

internet and create a bootable version of the operating system, a rescue disk that could be installed on a CD and that installation program is called an ISO. ISO.

Special Agent Shaver testified that an ISO is an image. It's an image file of the CD, a copy of a CD.

Your Honor, Special Agent Shaver testified that PFC Manning downloaded a Linux install, excuse me, rescue disk ISO multiple times and specifically on 2 March 2010 at 17:48:51 hours, 17:48:51.

He burned that Linux system operating, that Linux -- excuse me -- rescue disk operating system ISO to a CD on his personal map.

Your Honor, note Prosecution Exhibit 125. Prosecution Exhibit 125 is the disk utility log for PFC Manning's personal Mac and specifically lines 365 through 382.

THE JUDGE: That exhibit was what?

MR. FEIN: 125, and it's lines 365 through 382. This disk utility log from the personal Mac shows PFC Manning burning that Linux ISO to a disk.

You recall, Your Honor, that Special Agent Shaver actually used the exact same Linux ISO to view the folder contents that PFC Manning would have. The only way Special Agent Shaver explained that one could potentially obtain access to the SAM and system files was to boot the computer using this Linux operating system CD.

Now, Your Honor, you heard from Mr. Weaver, one of the primary authors of AR25-2, that under 25-2 bypassing includes finding capabilities that elevate the user's privileges.

He explained that traditionally bypassing means someone installed or modified a system in order to gain access in an unauthorized way, and this is exactly what PFC Manning did or at least attempted to do.

By equipping himself with Linux, a different operating system and booting the government SIPRNET D6-A computer using that CD, PFC Manning attempted to bypass and did actually bypass a network security system in order to obtain a security data.

Specifically, PFC Manning breached built-in security features within Microsoft Windows, the Army's approved operating system, on his D6-A computer that protected the FTP user account. He wanted the account log-in credentials to conceal his identity to continue abusing access to SIPRNET and classified information.

Special Agent Shaver testified that PFC Manning successfully obtained a portion of LM hash value for the FTP user account from his SIPRNET computer. And with that portion of the LM hash value in his hand, PFC Manning wanted a way to speed up cracking and decrypting the passwords for the FTP user account. So he turned to his two trusty sources for information, WikiLeaks and Intel link.

Your Honor, you'll see on page 6 of Prosecution Exhibit 123, these are the Assange chats, page 6. That on 8 March between 15:55 and 16:11 on 8 March between 15:55 and 16:11 PFC Manning chatted with Julian Assange and WikiLeaks and provided a hash value obtained from his SIPRNET computer SAM file.

With the direct assistance of Julian

Assange and WikiLeaks, PFC Manning attempted to reverse engineer the password for FTP user.

Your Honor, print 130, going back to a key piece of evidence in this case, is the summary created by Special Agent Shaver.

Your Honor, when you deliberate you'll have Prosecution Exhibit 130. Your Honor, with the direct assistance of JA WikiLeaks, he attempted to get the password.

Your Honor, take a look (inaudible).

On the top you have the extract from Prosecution Exhibit 123 the Assange chat.

On the bottom you have the EnCase forensic pole of what PFC Manning called and Special Agent Shaver testified a hex dot.

Special Agent Shaver created this summary showing PFC Manning's chatting with Julian Assange and the extract from the dot 22 SAM file. You can see the FTP user on the right side of the SAM file.

Your Honor, on the bottom right, FTP user shows up in that SAM file. And then following that is

the hashed algorithm. The hashed algorithm, Your Honor, is the 80C1049 all the way to the 351C. It's in a black bold on the left side of the FTP user.

He also testified that he conducted a process called a hex dump which converted the information on the SAM file to a hash value. On the left. Excuse me, Your Honor. On the left side is called the hex dump.

The reason that's important, if you look at the chats you will see that PFC Manning said at 1609 to Julian Assange, not even sure if that's the hash. I had to hex dump a SAM file since I don't have the system file.

And Special Agent Shaver, using EnCase forensics software, did the exact same process. As you can see, Your Honor, in black at the bottom left is that 80 number I just read.

Little difficult to see on these projections, Your Honor. It's clear on the document, Prosecution Exhibit 130.

And at the top of the chat, Your Honor,

PFC Manning inquires about KN hash cracking. Upon hearing about the rainbow table resource, he provides the partial hash values, confirming it's a SAM file origins.

What I mean by that is that that 80C1 number that is on the bottom left was provided by PFC Manning in his chats to receive assistance by Julian Assange in cracking his SIPRNET computer, the FTP user account information.

Your Honor, at 16:11:26 on 8 March 2010, within these chats as annotated here on PE130, Julian Assange responded that WikiLeaks, that is LM hash guide will handle, will pass it to his LM hash guide. That's on the second from the bottom from the right side.

Please note, Your Honor, that this chat occurred by PFC Manning was off shift, and in his CHU on his personal Mac, and this was at 16:11. Shift change occurred every day at 2200 just shy of 30 minutes at 22:28.

PFC Manning used his SIPRNET access to search for rainbow tables and Special Agent Shaver

testified that rainbow tables are used, are tables that are used in order to find known hash values for passwords if a known password in plain text converts to a known hash value. Fast way to quickly determine what that password is.

PFC Manning went to SIPRNET in order to figure out if he could find a rainbow table and he could not, but for six hours after he chatted with Julian Assange in order to find a way to get the FTP user account information, luckily for the United States PFC Manning did not find what he was looking for.

The accused successfully breached security protocols and obtained the portion of the hash value in the SAM file.

PFC Manning knew what to do in order to bypass the computer protocol and specifically, that is, specifically designed to protect the password information and he took deliberate steps to circumvent those protections by using a Linux rescue CD.

He violated regulation two ways. First, by booting the SIPRNET computer using a different

operating system, bypassed the security information security mechanism, the use of user name and password to gain access.

Special Agent Shaver, a normal user, did not have access to a file. You could only gain it by booting from a CD.

Second, by navigating the SAM file and obtaining part of the hash value of the password to the FTP user account, PFC Manning attempted to bypass the security mechanism in place.

Using Julian Assange and WikiLeaks, PFC Manning tried to figure out the password to another local user on his SIPRNET computer, one he did not normally have access to in the course of his work, so he could hide in plain sight and not operate under the potential fear of being caught.

Your Honor, I don't know if now is a good time to take a recess or I can keep going.

THE JUDGE: It probably is. 15 minutes.

MR. FEIN: Yes, ma'am.

THE JUDGE: Court is in recess for 15

minutes.

(Court in recess.)

THE COURT: Court is called to order. Let the record reflect all parties present when the court last recessed are again present in THE court.

Major Fein?

MR. FEIN: Your Honor, the next dataset are the GTMO documents, Specification 9.

Your Honor, the next set are the GTMO documents that serve as a basis for Specification 8 and 9 in Charge 2 and also, Your Honor, Specification 2 of Charge 3. Detainee Assessments Briefs, or DABs.

(Inaudible) PFC Manning researched GTMO information repeatedly on Intelink. He found the DABs in classified network and reviewed them.

He then discussed their contents with Julian Assange before exporting all the records in the database by using Wget, unauthorized program.

Even after PFC Manning stole them he couldn't stop talking about them with Adrian Lamo. It shows that he was looking to get the information

published with WikiLeaks from the beginning of his deployment.

He was looking for politically notable information that would garner as much attention as Reykjavik 13 did in February 2010.

Using the tools provided by him in the United States to analyze intelligence, PFC Manning searched for information that compromised to WikiLeaks when he found the GTMO DABs, detainee assessment briefs.

Your Honor, what are DABs? DABs are a recommendation to the US SOUTHCOM commander for the disposition of detainees, which included the detainee's threat level and intelligence value to the United States.

The DABs contain classified information pertaining to United States intelligence regarding terrorists and their organizations and classified information about terrorist training, TTPs, and intelligence analysts of terrorist organizations.

Furthermore, Your Honor, the DABs

demonstrate the US intelligence gaps with terrorists and terrorist organizations and the extent of cooperation with the United States.

Rear Admiral David Woods testified as the OCA for the DABs that compromising the DABs could cause serious damage to National Security and thus they are classified at the secret level.

THE COURT: Who was the person?

MR. FEIN: Rear Admiral David Woods, the previous demander of JTF GTMO.

The DABs are housed in three locations, all of which are classified.

Mr. Moats, Your Honor, he testified as a head of the DAB branch that the DABs are stored locally on the GTMO share drive on SIPRNET, on the JDIMS-I, a unique system for the JTF GTMO, and also on SIPRNET on Intellipedia.

Mr. Moats testified that the DABs are stored by document ID number and a user can see the document ID number by scrolling over the link for each DAB on Intellipedia web page.

Your Honor, on 8 December 2009 PFC Manning first accessed the DAB website.

On 5 March --

THE COURT: What was the date?

MR. FEIN: 8 December, 2009.

Your Honor, 5 March 2010, the Intelink logs show that he attempted to download the entire database but could not complete that download. Prosecution Exhibit 82 shows PFC Manning's manual attempts to collect the DABs.

Special Agent Shaver testified that PFC Manning started downloading DABs using the right click save method, as an ordinary user would on 5 March 2010. And Special Agent Shaver testified that the right click method was slow and wrought with errors.

THE COURT: Exhibit 82?

MR. FEIN: Your Honor, Prosecution Exhibit 82 is an extract of the Intelink log activity for 5 March 2010, Your Honor, line 4 of Prosecution Exhibit 82 shows PFC Manning's attempt to download one DAB at 3:22.

Why is this important, Your Honor?

Because the summary shows that PFC Manning failed in this attempt because on the Intelink log data there's a 000 code at the end of the actual web address, 000 code. Again Prosecution Exhibit 82.

Special Agent Shaver testified that the 000 code signified that the download did not go through. It was not complete.

A minute later PFC Manning successfully downloaded the same data. Special Agent Shaver also explained in a attempt that was successful a download was successful if the code 200 showed up next to the web address. So 000 failure; 200 complete.

On just the first page of Prosecution Exhibit 82 there are 23 attempts to download DABs, 12 attempts were not successful with 000 code.

In order to get 11 successful downloads PFC Manning spent approximately 7 minutes according to the Prosecution Exhibit 82, Your Honor, in order to increase the (inaudible), PFC Manning turned to an unauthorized program, Wget.

Special Agent Shaver testified that Prosecution Exhibit 157 shows PFC Manning searching for information on how to make Wget run faster and that was on 7 March 2010.

Special Agent Shaver testified that PFC Manning began running Wget from dot 22 computer system on 7 March 2010 the first time and PFC Manning introduced that software onto his classified computer in order to do that.

Your Honor, the unit AUP, authorized user for which Captain Tripp (inaudible) will remember testified prohibited soldiers from executable code which specifically includes dot EXE files to a DoD computer.

And you'll remember from the testimony Special Agent Shaver, Your Honor, dot EXE files are executable files.

Programs downloading the unauthorized Wget EXE file violated AR25-2 paragraph 4-582 as detailed in Specification 2 of Charge 3.

As Special Agent Shaver testified PFC

Manning, after downloading Wget dot EXE, had to program Wget, how to operate Wget, did not have a graphical user interface or GUI, therefore it was not as simple as double clicking an icon of an installed program on the D6-A computer and running it.

Your Honor, explained here is Prosecution Exhibit 189, page 1. This is the help file Special Agent Shaver testified he extracted from PFC Manning's computer. When I type in Wget-H, this help file displays in an MS dot prompt. Because Wget is a command line tool, it has many options as displayed on page 1 here.

PFC Manning had to research how to program Wget and how to program it in order to harvest the entirety of US SOUTHCOM database of DABs. PFC Manning used the document ID number, the unique database identifier in Wget to extract those DABs.

Your Honor, PFC Manning was able to download the database in less than four hours once he was able to get Wget running, whereas his manual attempt on 5 March had been plagued with errors. PFC

Manning's success rate with Wget on 7 March was much better.

Mr. Johnson testified that while PFC Manning was harvesting those DABs, he also was talking to Julian Assange through his chats and he recorded that information.

Your Honor, PFC Manning and Julian Assange discussed the value of the DABs, the types of information in the DABs, and the status of the uploads.

That is in the Assange chats pages 3 through 5. Pages 3 through 5.

Two months after stealing the DABs, PFC Manning bragged, telling Mr. Lamo that, oh, the JTF GTMO papers Assange has those, too. PFC Manning went so far as to characterize the DABs as a highlight on the information he stole.

On 25 April 2011, WikiLeaks released purported DABs on their website. Prosecution Exhibit 95 are the charged DABs in this case.

Your Honor, Prosecution Exhibit 95 showed that the DABs are marked secret on the top and bottom

of each page. WikiLeaks published the DABs because they had not been publicly released at that point and the information in the DABs was not available anywhere else.

The evidence from all the witnesses indicated that the documents were closely-held.

As a defense's witness Colonel Retired Davis testified Defense Exhibit Victor, which is a DAB, was not necessarily useful to a prosecutor who needed the underlying evidence but Defense Exhibit Victor was an executive summary of that evidence and the intelligence reporting contained little public information.

When PFC Manning extracted the DABs to his personal computer, he completed the (inaudible) of those records. The DABs that were stored on the classified system with only authorized personnel with a need-to-know could access them. At no time, Your Honor, was PFC Manning authorized to house those records on his personal laptop.

Furthermore, Your Honor, PFC Manning

converted the information in the DABs when he conveyed them to WikiLeaks for publication.

PFC Manning specifically intended for the DABs to be published and WikiLeaks obliged.

The United States devoted significant resources to protect the classified information in DABs from actual compromise.

Mr. Lewis testified that foreign intelligence services will pay for the information precisely because its exclusive possession provides a significant benefit to the United States.

The publication of the DABs completely deprived the United States of the exclusive possession of the use of that information, exclusive use.

Accordingly, Your Honor, by causing the DABs to be published, PFC Manning substantially interfered with the United States' ownership rights in those records.

Using Wget he scraped an entire classified website. PFC Manning then placed the exported classified records on his personal computer. After

transferring the records to the personal computer he talked about GTMO records with Julian Assange, as I described before, as he delivered them to their web sites online submission program.

Your Honor, in the end, PFC Manning felt the GTMO documents were the highlight and were among many records he admitted to stealing.

Mr. Moats testified that each DAB, as the chief of the DAB branch, was the product of 80 to 90 hours of work by intelligence professionals, each DAB, Your Honor. And Mr. Moats testified that the lowest ranking person that worked on the DAB creation had the grade of E4. A specialist of the United States Army in 2005, a specialist or E4, earned $1,500 approximately per month in base salary.

Assuming 40 hours per week, that works out to an hourly wage of about $9, Your Honor.

PFC Manning stole over 700 detainee assessments. Mr. Moats testified that each DAB took approximately 80 hours of work, thus 56,000 hours were spent creating those DABs. Therefore, the cost to

create the DABs was at a minimum $525,000 which is based off 56,000 hours at the lowest grade of a producer of the DABs at $9.39 per hour.

Your Honor, additionally, DABs are valuable to foreign intelligence services.

Your Honor, at this time United States requests that the accused and Major Hurley relocate to the witness box and I will hand Appellate Exhibit 617 to the Court and the Defense.

Your Honor, Mr. Lewis testified that the foreign intelligence services in multiple countries actively seek information contained in DABs and would pay for DABs for the US SOUTHCOM database.

The foreign intelligence services seek information pertaining to GTMO counterterrorism efforts as detailed in Classified Reason Number 7.

Mr. Lewis testified that country 4 would pay over $7,000 for the records in the US SOUTHCOM database and Mr. Lewis called the valuation conservative as set forth in Classified Reason Number 8.

Your Honor, I'm going to transition over to the two OJ documents that service the charged documents for Specification 3 of Charge 2, and if I may request that PFC Manning and Major Hurley stay in their current position with the classified documents for the beginning.

Your Honor, PFC Manning knowingly compromised the documents belonging to United States intelligence agency that makes up Specification 3 of Charge 2.

I will generally discuss in this open session the proof the United States presented for the OJ information, however the United States primarily refers the Court to specific -- to the top portion of Appellate Exhibit 617 before I continue as that is a classified legend for the remaining portion of this argument.

THE COURT: Okay.

MR. FEIN: Your Honor, the United States does not intend to specifically reference any of that information again at this point so the United States

request that PFC Manning and Major Hurley relocate and we could retrieve Appellate Exhibit 617.

Your Honor, the charged memoranda were published on US official website on the dates dated in print 1807 paragraphs 14 and 16. Prosecution Exhibit 180 paragraph 14 and 16.

Line 425 of Prosecution Exhibit 81, the Intelink search logs, reveals that the accused searched for the equity holder of these documents on a SIPRNET computer on 9 March 2010. That's line 425 Prosecution Exhibit 81.

According to the testimony of Special Agent Shaver about the specific portion of the file named index dot data mining on PFC Manning's dot 22 SIPRNET computer, the memoranda were likely present on the dot 22 computer around March 2010.

Special Agent Shaver created Prosecution Exhibit 154 to show this migration of the file names during his closed session testimony.

THE COURT: What exhibit is that?

MR. FEIN: Prosecution Exhibit 154.

As a reminder, Your Honor, the index dot dat file is a file that captures the internet history of files moving between web pages and on the computer.

Special Agent Shaver testified that he could tell that the memoranda were on the machine by looking at an excerpt of the index dot dat file which is a file used, as I just mentioned, to record the web sites and files accessed in Microsoft Internet Explorer.

According to Prosecution Exhibit 154, PFC Manning downloaded the first memorandum on 17 March 2010. He saved the first memorandum and the second memorandum to his desktop in the Bradley dot Manning profile in his My Documents folder on the dot 22 computer and that was on 21 March 2010.

Both documents that he download were PDF file names very similar to the names of the memorandum. All this is reflected in Prosecution Exhibit 154.

Special Agent Shaver testified that most memorandum were moved to the folder named Blah, B-L-A-H, on 22 March 2010. Both memorandum were moved

to a folder named "Interesting." The name of the folder itself -- was -- the name was "Interesting" on that same day, Your Honor.

About 30 seconds later, Blah dot zip file name was created in Bradley dot Manning's My Documents folder.

According to Mr. Johnson in the volumes dot txt document, that's Prosecution Exhibit 127, a file named Blah dot zip was placed on the accused's personal Macintosh computer on 22 March 2010.

According to Mr. Johnson, blah dot zip was burned from a Windows machine onto a CD at 12:55 on 22 March and that's reflected again on Prosecution Exhibit 127.

The charge memoranda, Your Honor, were properly marked classified. The memoranda also contained national defense information as articulated in Prosecution Exhibit 180 Alpha and 181 Alpha. Paragraphs 12 through 18.

Specifically they both contained information that concerns intelligence activities,

sources and methods and US foreign relations and activities such that an authorized disclosure of these memoranda, Your Honor, reasonably could be expected to harm or cause serious harm to the national defense and foreign relations of the United States.

Prosecution Exhibits 180 and 181 Alpha also explained how the information contained in the memoranda would be useful to the enemy if released and show that the information in the memoranda is true, at least in part.

The dates the memoranda were posted on WikiLeaks are recorded in Prosecution Exhibit 180. Prosecution Exhibit 180 paragraphs 15 and 20.

These paragraphs also state that these memoranda were never otherwise released outside the classified United States Government official channels.

According to Prosecution Exhibit 141, the open source logs for bradass87 between 9 April 2010 and 13 April 12010, PFC Manning looked at several documents on the open source center about the reaction to release some of this information.

PFC Manning searched for the information on the SIPRNET computer. He saved it on his dot 22 computer. He moved it to his personal Macintosh computer and then the memoranda were posted on WikiLeaks.

Later, PFC Manning accessed the information to read about the fallout.

The evidence shows that the accused had reason to believe that the information could be used to injure the United States to the advantage of a foreign nation.

Your Honor, the next dataset is the Net-Centric Diplomacy database and the cables contained within. This goes to Specifications 12 and 13 of Charge 2 and also Specification 2 of Charge 3.

The Net-Centric Diplomacy database contain decades of classified closely-held United States cables related to foreign policy, including sources of intelligence, Your Honor.

PFC Manning began by compromising a single cable, Reykjavik 13 because he thought it would be of

interest to join Assange, WikiLeaks, based on its subject matter at the time and focus on Iceland.

PFC Manning was correct. After PFC Manning stole the cable and WikiLeaks published it, PFC Manning claimed that the affect was a recall of an ambassador.

Having seen the result of his actions, PFC Manning saw an opportunity for more notoriety.

Thereafter, PFC Manning set about to compromise the entire NCD database, Net-Centric Diplomacy database.

Instead of helping his unit, PFC Manning took the opportunity to harvest over 250,000 Department of State cables for release on WikiLeaks and to the world.

Ms. Tann testified that a cable is an official message of the Department of State and cables can be sent between posts and the Department of State headquarters in DC.

Ms. Tann testified each cable contained a message resource number, which is a unique identifier. Cables are used for communicating and conducting United

States foreign policy.

Accordingly, cables are often classified and contain sensitive information and information that must be closely guarded to enable the United States to conduct its foreign policy effectively.

Your Honor, Prosecution Exhibits 169 Charlie through 177 Charlie, these are the Charlie subexhibits for 169 through 177, these are the charged cables, are examples of compromised cables as they appear on the Net-Centric Diplomacy database. Each cable and NCD contained a warning banner describing the limited extent of the user's authorization to view each cable.

Your Honor, Prosecution Exhibits 169 through 178, the Alpha series of all of those, 169 through 178, Department of State officials described the contents of the stolen cables. The cables contained PII, such as names and the sources of the information, as well as the originator of the cable itself.

Using names the cables identified meetings

with sources, human rights activists and others at risk of incarceration, torture, or death in the country of origin.

The cables also reveal sensitive information regarding foreign relations, intelligence sources and methods, diplomatic relations and foreign policy.

Special Agent Bettencourt testified that the purported cables posted on WikiLeaks.org span decades with dates from 1966 up until 2010.

And Mr. Murphy testified that the charged cables, that's again Prosecution Exhibit 169 through 177 and it's the Charlie series, contained information that if compromised could cause harm or serious harm to the National Security. He was a duly appointed OCA who testified that the cables were either secret or confidential.

Your Honor, why did the Department of State create NCD? Ensuring the information and intelligence in cables took on increased importance after September 11.

Mr. Weiss Carter, he testified that acting on the need for intelligence sharing the Department of Defense providing Department of State funding to make it necessary the information available on SIPRNET.

As a result of that funding, NCD was created to share information to all users on SIPRNET.

Mr. Weiss testified that NCD was a system that was specifically designed to provide the Department of State in the SIPRNET community with access to diplomatic reporting to ensure there was information sharing across the Government at all levels from priorities to generalities.

Thus, Mr. Weiss testified that NCD resided only on SIPRNET and J links.

Captain Lim testified that he sent an e-mail telling his soldiers that NCD could be used to accomplish the mission in the S2 shop.

Captain Lim testified the 210 mission was to train, mentor, advise and assist Iraqi security forces in Southeast Baghdad.

Captain Lim testified that NCD was useful

for that mission in Southeast Baghdad but not for Iceland, information pertaining to Iceland, South America, Asia or the rest of the globe.

Mr. Madaras testified that he never used NCD as a 35 fox because his focus was on the 210 area of responsibility and that was in Baghdad.

PFC Manning's focus should have been on the same areas of operation as a shared analyst.

Your Honor, instead was using NCD to accomplish his mission and support his fellow soldiers as an all-source intelligence analyst, PFC Manning chose to harvest decades worth of SIP disk, SIPR distribution cables, to gain his notoriety.

In his chats with Mr. Lama, PFC Manning thought he was smart enough to know what's going on in the world.

The day after returning from R and R leave and on 15 February 2010 that's when he compromised Reykjavik 13 and having observed the results of stealing and disseminating that information, PFC Manning went to work on reaping more cables.

From late February to early March 2010 PFC Manning worked on engineering a method to steal the entirety of the NCD database.

Your Honor, note that Mr. Carter testified that a user of Net-Centric Diplomacy can only access cables through the Net-Centric Diplomacy database web page interface on the Department of State web page.

Mr. Weiss also testified that access to cables on Net-Centric Diplomacy was limited because NCD allows a user to view through a web browser or print a single cable, save a single cable at a time.

When asked why there's no technical restrictions put in place on NCD outside of the web browser requirement, Mr. Weiss answered that it would inhibit sharing of information, be administratively difficult to manage, if not impossible.

Captain Lim also testified that an NCD user can access NCD through a website, a user searched for cables using key words on the NCD web page.

He testified it did not have an export function similar to what CIDNE had, click a button and

export 30 days at a time. And he did not save cables. He only read them for information related to his mission.

Your Honor, Special Agent Shaver testified that NCD was accessible only through a web page and the only way to access a cable was to type in the information in the search bar, click search, wait for your return to come up on the web page then click the specific cable in your web browser and once the cable comes back it views in the web browser and at that point you can save or print.

Essentially you're pointing and clicking.

Mr. Weiss also testified NCD did not allow for batch downloading. Using NCD as a normal user, PFC Manning never could have accessed let alone downloaded over 250,000 cables.

As Captain Lim and Special Agent Shaver testified, NCD only allowed a user to view one cable at a time using a web browser to view a web page. This was a system limitation that PFC Manning understood and had to bypass to accomplish his own personal task.

PFC Manning knew he could not physically download over a quarter million cables manually with NCD's organic functionality typing in 251,000 cables into a search bar, clicking on each individual one and right clicking to save or print.

So he turned to what he knew best from his experience with the GTMO DABs, Wget.

And, Your Honor, turning to Wget PFC Manning exercised a self-help remedy in order to prepare a method for his compromise, or his exfiltration as PFC Manning had actually called it in his personal tasking order for the GAP. His personal tasking order for Department of State information to create, as he said to Adrian Lamo, worldwide anarchy.

Your Honor, that's Prosecution Exhibit 30. The Lamo chat, page 9, his goal to create worldwide anarchy.

PFC Manning began by searching for Wget, again, prosecution Exhibit 157 shows that PFC Manning searched for Wget on his NIPRNET computer and Special Agent Shaver testified that the search related to Wget

on 7 March 2010 was a search to figure out how to make Wget run faster.

On both 7 March 2010 and 27 March 2010 PFC Manning used Google to search for the executable file Wget.

Then, Your Honor, as shown on Prosecution Exhibit 157, PFC Manning downloaded Wget onto his NIPRNET computer.

Special Agent Shaver testified that Wget was in PFC Manning's users account in March of 2010 and introduced again in May of 2010.

Your Honor, Special Agent Shaver testified about Wget. Wget was an executable file that had been copied and placed in the My Documents folder on PFC Manning's dot 22 SIPRNET computer.

We know Wget was run from PFC Manning's computer because of the PreFetch files, the Microsoft Window files that save, say, a slice of the program from memory when it runs and that slice includes the exact location on the hard drive or, as Special Agent Shaver called it the path, the address on the hard

drive for which that file ran.

And each time a different version or each time Wget is run from a different location, a different PreFetch file is created.

Your Honor, Prosecution Exhibit 188, 188 shows the PreFetch files for Wget and all of the locations on PFC Manning's computer that he ran Wget.

Your Honor, it's clear that Wget was not run by PFC Manning from a disk. So why did PFC Manning have to copy Wget to his computer and run it to obtain the state cables?

This is very simple, Your Honor.

The Net-Centric Diplomacy database was only accessible by using a web browser, opening the web page, typing in the search term and clicking the search results.

Then the user had to navigate to the web browser, decided which cable he wanted to view, click that cable, wait for the cable to load in his web browser and once it loaded he would have to decide whether to print or save.

Your Honor, PFC Manning knew that. And he knew the process. That process, the NCD in a D6-A computer required was not fast enough or efficient enough to afford him the option to harvest over 250,000 cables in such a short period of time.

In fact, Mr. Weiss testified, as I mentioned earlier, that NCD database did not have a function that allowed for mass downloading. So PFC Manning did, as I said before what he did best, he used Wget to bypass the NCD web page and go directly to the web server to scrape all the Department of State cables directly from the web server.

Your Honor, Prosecution Exhibit 187 was the demonstrative aid that Special Agent Shaver testified about how PFC Manning used Wget.

Special Agent Shaver testified that PFC Manning used Wget on his computer, the bottom left, and rather than going straight up to the web page click search, wait for the results to come up and then save, he went directly using Wget onto the web server and was able to mass download all of the Department of State

cables from that database.

What that allowed, Your Honor, PFC Manning to do was to circumvent, to bypass the exact mechanism and place on this computer system the restrictions put in place of using a web browser in order to view these documents and in order to go grab them and bring them down to his computer.

In order to accomplish this complex task of running Wget, PFC Manning had to take specific steps to prepare.

First, get and copy and paste the list of the MRNs, the unique identifiers from the database from the web page to itself. So he had to query, as Special Agent Shaver testified, the newest cables published, copy all the MRNs, copy, paste and then pasted them into Excel.

Second, PFC Manning used Microsoft Excel to automatically link together in a chain the MRNs that he pasted into a Wget command line that he used the Wget help file to figure out.

Actually, Special Agent Shaver used the

term catenate organic function that PFC Manning had to program in order to make this process to occur quickly and ultimately for 251,000 plus cables.

Finally, PFC Manning copied and pasted those lines from the Excel spreadsheet with the Wget commands into what Special Agent Shaver testified were batch files. A batch file allows you to run a executable program rapidly over and over again.

And Special Agent Shaver testified about the different batch file extracts he found on the dot 22 computer.

Your Honor, PFC Manning used Wget to create a functionality that did not exist.

Whereas Mr. Weiss testified the user accessed a single cable using a web browser, PFC Manning accessed over a quarter million cables by introducing Wget.

He harvested those cables using Wget in its command prompt without any action in the NCD graphical user interface.

Prosecution Exhibit 159, Your Honor, shows

the staggering number of connections to the Department of State cables servers and the firewall logs.

Prosecution Exhibit 159 shows that PFC Manning's computer connected to the Department of State cables firewall more than 700,000 times between 28 March and 9 April; 700,000 times between 28 March and 9 April.

PFC Manning spent all of his working hours over 10 days harvesting cables for the transmission to WikiLeaks.

Prosecution Exhibit 159 also shows that his computer connected to the same firewall over 53,000 times on 3 May 2010 that's when PFC Manning went back to the NCD to harvest cables from March 22 onward.

Mr. John testified that PFC Manning's personal computer possessed a script, a program that could convert information from a cable into what's called Base64 format.

Your Honor, Base64 is an encoding layer that condenses information to a simpler form to transmit over the internet. The script had fuel for

both classification and message record number.

Undeterred by system restrictions and limitation, PFC Manning had harvested as much information as possible in the shortest amount of time and thus he had to reintroduce Wget onto his computer at this time.

So at the end of his nearly two-week mission in March and April 2010, PFC Manning had harvested more than 250,000 cables.

The evidence showed that he harvested those cables and packaged them and compressed them into Base64 for transmission to WikiLeaks.

Your Honor, Prosecution Exhibit 102 is a printed version at the very top of the worksheet named the backup xlsx file that was left on the dot 22 computer. Backup dot xlsx. This is a Microsoft Excel file.

Your Honor, that printed worksheet, Prosecution Exhibit 102 shows how PFC Manning cataloged every single cable he harvested from NCD. The first line on that worksheet, Your Honor, is 251,288.

Your Honor, I'll talk about that number in a moment. But Prosecution Exhibit 104 that shows backup dot xlsx, that was created on 3 May 2010 and that's in that bloop folder we have talked about.

THE COURT: Created when?

MR. FEIN: 3 May 2010, Your Honor.

And that was in the bloop folder in PFC Manning's My Documents.

Prosecution Exhibit 104 also showed that files dot zip, another file was created on 4 May 2010.

The volumes dot txt, the volume mounting data from the SIPRNET computer shows Prosecution Exhibit 127, shows that, Your Honor, the volume dot txt file show that a file named file dot zip was burned to a CD on a SIPRNET computer that same day, 4 May 2010, and ultimately moved to PFC Manning's personal Mac.

Your Honor, on 31 August 2011 WikiLeaks published 251,287 purported Department of State cables without any redactions. That number is very important. I stated earlier PFC Manning left behind a file --

THE COURT: What was the number?

MR. FEIN: 251,287, Your Honor.

THE COURT: Okay.

MR. FEIN: And, Your Honor, if you recollect, the backup xlsx file started with the number 251,288.

While WikiLeaks published the 251,287 purported cables that were dated through February 2010, the purported cables WikiLeaks released did not include March, April and May 2010.

PFC Manning had the cables from March through May 2010 ready to go with his starting number and that backup dot xlsx file of 251,288. And those were the cables, Your Honor, located in the files dot zip file that Special Agent Shaver testified.

This number of course, 251,288, is the next number in line after 251,287. That is -- so ultimately, Your Honor, PFC Manning, PFC Manning reintroduced Wget to go back and harvest the remaining cables starting with 251,288 because he had already compromised to WikiLeaks 251,287 purported cables that they released unredacted.

His determination and persistence had not ceased. He wanted more to increase the effect in his future right at this time. When extracted the records from NCD to his personal computer, PFC Manning completed the theft of those records.

The NCD records were stored on a classified system where only authorized personnel with need-to-know could access them. At no time was PFC Manning authorized to house those records on his personal computer.

Furthermore, PFC Manning converted the information in the cables from NCD when he conveyed them to the WikiLeaks for release.

PFC Manning specifically intended for the cables to be published and WikiLeaks obliged. The United States devoted significant resources to protect the classified information within NCD.

Mr. Lewis testified that foreign intelligence services will pay for information precisely because its exclusive possession provides significant benefit to the United States.

By causing the cables to be published, PFC Manning substantially interfered with the United States' ownership rights of exclusive possession of that classified information in the records.

Your Honor, the United States requests that the accused and Major Hurley relocate to the witness stand and I will hand Appellate Exhibit 617 to both the Defense and the Court.

Your Honor, Mr. Lewis testified that the foreign intelligence services of multiple countries actively seek information contained in the Net-Centric Diplomacy records and would pay for records from the Net Centric Diplomacy Database.

The foreign intelligence services seek information pertaining to United States strategic plans and specific geographic areas as detailed in Classified Reason Number 5.

Mr. Lewis testified that country 3 would pay well over $1,000 for the records in the Net-Centric Diplomasy database as set forth in Classified Reason Number 6.

Mr. Lewis testified that he conducted a search of the Net-Centric Diplomacy data by using specific groups of key words. Based on his search he received 900 responsive hits. The hits constituted 900 separate documents or cables.

Mr. Lewis testified that country 3 would pay over $2,000 per document related to the searched key words.

Therefore, Your Honor, according to Mr. Lewis, the Net-Centric Diplomasy database is worth over $1.8 million to foreign intelligence services.

Your Honor, the United States retrieves Appellate Exhibit 617 from the Defense and the Court.

Now, Your Honor, what about Wget? PFC Manning knew that he was not authorized to introduce Wget on a Government computer.

Chief Ehresman testified that soldiers aren't allowed to introduce programs on their computer. They're allowed to run a program on a CD with authorization of the both Chief Ehresman and Mr. Milliman testified that if a user wanted to add

software, the user would have to check with Mr. Milliman for approval.

Mr. Milliman, a D6-A contractor, testified that he told the entire unit during a shift change brief in the first month of deployment that he owned the computers and was the proper authority.

Your Honor, the first month of deployment for PFC Manning would have ended, the first full month would have ended at the end of November, Your Honor, well before March 2010.

Ms. Florinda White testified that Wget was not authorized for D6-A computers.

Mr. Kits also authorized -- testified that Wget was not authorized.

PFC Manning introduced the Wget program without requesting authorization.

Wget was unlike any other program that was openly used by soldiers in the SCIF. No one else even knew what it was or what it was capable of doing that came and testified here in this court martial, Your Honor.

So when does the Army allow Wget on its networks, Your Honor?

Well, Chief Royer testified, I'm sorry, Your Honor, to correct what I just said, no one from 210 Mountain that was deployed in Iraq at the time had ever heard of Wget including, Captain Cherepko and Mr. Milliman when they were deployed.

You did hear, Your Honor, from Chief Royer who testified that Wget is used in his op 4 capacity for attacking Army networks. He uses Army Wget to attack Army networks. And that's only in circumstances that he's ever been authorized to introduce Wget to a Government computer system. He did penetration testing.

Chief Royer further testified that Wget can be used in spear phishing and social engineering attacks and both Captain Cherepko and Chief Royer said Wget scrapes entire web sites and can choose any data that it chooses to extracts.

Your Honor, Mr. Weaver testified, he was one of the main authors of 25-2, he testified that

introducing unauthorized software violated 25-2.

Mr. Weaver testified that the authority to add software is reserved to specified administrators. PFC Manning did not have administrator privileges on any of his computers.

Mr. Weaver testified that introducing software or creating elevated privileges constituted a bypass of authorized mechanisms. He testified that only automated functions a user possessed were those that came and were installed on the system as authorized by the Army.

He testified that a commander could authorize music and games on a computer system. Mr. Weaver also testified that a user had personal responsibility under 25-2.

Finally he testified that a user couldn't add executable files or Wget specifically under AR25-2.

Your Honor, as Mr. Kits, expert on D6-A testified that one program that soldiers did use mIRC chat, had been authorized as part of a technical bulletin that gave commanders the authority to use the

program.

Colonel Miller testified in regard to 210 Mountain's use of mIRC chat as part of the mission.

Colonel Miller testified that music, movies and games would have (inaudible) morale and to the best of his knowledge were not self-executable files.

There's been evidence, Your Honor, of movie files to include music, movies and games from the T-drive, the share drive the brigade staff used; but there has been no evidence through testimony or otherwise admitted that music, movies and games were actually introduced to the T-drive or to any SIPRNET computer by any particular soldier.

There has been no evidence presented that movies, music or games are executable programs.

Additionally, there's been no evidence that storage of movies, music and games were prohibited. Just the introduction, the introduction is what AR25-2 regulates. Introduction of music, movies and games onto a computer system when they're not authorized is prohibited.

Mr. Weaver testified that there is a significant distinction between introduction and storage of files according to the regulation.

Mr. Weaver distinguished this for moving files already on a network like the T-drive because moving files is traditionally authorized under AR25-2.

While movies, movies and games and authorized programs like mIRC chat were actually authorized by the commander, Wget was not. As stated before, was unknown to every single witness who testified and was in Iraq and FOB Hammer at the time PFC Manning was there.

Your Honor, and how PFC Manning used Wget informs the knowledge that he knew it was unauthorized. He used Wget in secret. He never asked for permission to use Wget.

And Chief Royer testified that someone could not even see Wget from five feet away. It's a command prompt run program.

Special Agent Shaver testified that Wget could be run in the background.

Chief Royer testified that unlike mIRC chat that has a window with chat rooms on it, no one who has never seen Wget before would know what it is.

And Sergeant Sadtler, Your Honor, he testified that PFC Manning had the habit of locking his screen to hide what he's doing on his computer even when he was still sitting at his computer if another individual walked up.

Your Honor, the United States is not arguing that PFC Manning was prohibited from accessing the NCD database itself or from downloading individual cables through the NCD database interface.

However, PFC Manning was only authorized to do so through using a web browser installed on his D6-A SIPRNET computer because that is the tool, the program the United States Army gave him to accomplish that mission and he was not authorized to install or copy any other programs onto his computer.

He copied Wget onto his computer for one purpose and one purpose only, and that was to access the NCD web server directly and scrape it for all the

Department of State cables.

Your Honor, the next set of specifications and the dataset is the Farah investigation. This is Specification 10 of Charge 2. Specification 10 of Charge 2.

Your Honor, earlier you heard that PFC Manning began helping WikiLeaks in late 2009 when he compromised the video BE22PAX.wmv, the Gharani airstrike video. The video, the military operation in the town of Gharani and the Farah province of Afghanistan. That military operation resulted in US CENTCOM conducting a formal investigation into the circumstances surrounding the civilian casualty incident. The United States stored that investigation in a folder named Farah on the (inaudible) that is only available on SIPRNET. BE22PAX.zip and wmv was located in the video subfolder.

Your Honor, four months after compromising BE22PAX.zip and the video within it, PFC Manning returned to the Farah folder located on the CENTCOM SJ web page to download and compromise the remaining

documents related to that investigation.

Special Agent Shaver testified that on 10 April 2010 PFC Manning visited Farah folder. Within 2 hours PFC Manning had downloaded more than 330 investigative files from the Farah folder onto his SIPRNET computer.

Your Honor, Prosecution Exhibit 129, 129 is an excerpt of the CENTCOM SharePoint logs showing when PFC Manning downloaded the documents from the CENTCOM website.

Your Honor, Prosecution Exhibit 128 is a summary of the portion of index dot dat file on PFC Manning's SIPRNET computer showing many of the documents PFC Manning downloaded from the CENTCOM website on the SIPRNET computer.

As I explained earlier, Your Honor, Prosecution Exhibit 128 shows PFC Manning's computer connecting to the SharePoint server and the Prosecution Exhibit 129 are the SharePoint logs showing PFC Manning or showing files being downloaded.

As noted earlier, Special Agent Shaver

testified that PFC Manning did not take the video titled BE22PAX.zip and wmv or any other zip file on 10 April 2010. No files were downloaded that day from the CENTCOM website. Why not?

United States argue it's obvious. He had already done it, taken the videos. Why did he wait until 10 April 2010 to download and compromise the documents related to military operation? Why decide in 10 April 2010?

Your Honor, it's during this time from starting 5 April 2010 to be exact that WikiLeaks released Apache video between 7 and 10 April 2010 and the annotated and Prosecution Exhibit 81 the Intelink search logs, specifically lines 628 through 640, 628 through 640. PFC Manning searched Intelink for WikiLeaks 11 times and 'Collateral Murder' twice.

He was monitoring and reveling in the reaction to the Apache video.

Your Honor, PFC Manning saw the rippling effects caused by the release of the Apache video less than a week earlier and he craved the same effect of

that Gharani military operation especially considering WikiLeaks had the video since before Christmas and hadn't released it yet. PFC Manning knew the charge documents for Specification 10 were classified. These documents were probably marked secret.

Of the 10 charged documents consisting of 141 pages, 90 pages are marked secret at the top and bottom and a total of 504 classification markings, including the paragraph markings, appear in total.

Your Honor, the documents were located on the SIPRNET on the CENTCOM SharePoint page as explained earlier with respect to the compromise of the video. Each of these web pages had a secret banner across the top that said "secret" multiple times. When the user scrolled down in the video, each page had that same secret banner.

Your Honor, Mr. Hall, former intelligence analyst and expert testified that intelligence analysts are trained to handle classified documents according to their classification markings and that only an OCA is in a position to say otherwise.

Further, many former unit colleagues of PFC Manning testified that their trained practice is to treat information on SIPRNET as classified.

Your Honor, even PFC Manning's two non-disclosure agreements that he signed specifically state that if he's uncertain about the classification and status he is required to assume it's classified unless he's told otherwise by competent authority.

The charge documents for Specification 10 relate to the national defense of the United States, Lieutenant Commander Hoskins and Mr. Neri, excuse me, Lieutenant Colonel Retired Neri, both testified that the charged documents contained the type of information which can cause serious harm in national security and thus should be secret.

And then Rear Admiral Harward, the deputy commander of US CENTCOM, and an OCA, testified that all the documents were properly classified at secret level.

Your Honor, multiple witnesses testified that the charged documents contained TTP, troop movements, close air support, troops in combat,

graphics showing troop movements, operational activities, weapon systems and code words.

And finally, Your Honor, the United States Government has never made those documents of the Farah investigation, the classified documents, available to the public.

Your Honor, the Global Address List Specification 16 of Charge 2, also Specification 3 Charge 3, excuse me, Your Honor, Specification 4 Charge 3. Your Honor, there's no coincidence that on the same day of having PFC Manning's SIPRNET connection severed --

THE COURT: Which specification did you say is Charge 3?

MR. FEIN: Specification 4, Your Honor.

Your Honor, it's no coincidence on the same day having the SIPRNET connection severed by being removed from the SCIF that WikiLeaks set out a net call for as many dot mil e-mail addresses.

7 May 2010 we would like a list of as many dot mil e-mail addresses as possible. Please contact

the editor@wikileaks.org or submit.

Your Honor, PFC Manning saw this 2008 and jumped at the opportunity to continue disclosing closely-held information to WikiLeaks. Especially after being removed from the area with readily available SIPRNET.

Special Agent Williamson testified that shortly after the 2008 was published on 7 May, PFC Manning searched for macros to extract the GAP.

What does that mean, Your Honor? He searched for a process in order to extract the GAP. And by 13 May, PFC Manning had extracted Global Address List and deleted the stolen files.

Specification 4 of Charge 3 accounts for this criminal misuse of the NIPRNET and Global Address List information system and Specification 16 is the theft of the Global Address List for his own personal use.

Your Honor, Specification 4 of Charge 3 charges PFC Manning with violating AR25-2 paragraph 4-5A3 by using an information system in a manner other

than its intended purpose.

According to AR25-2 information systems includes computers as well as set of information resources like the Microsoft exchange Global Address List.

Chief Nixon testified that the GAL is a US Government product which populates information at the organizational level ultimately listing every person, entity, and machine within a given domain, and in this case it's Iraq. It is the interface Outlook users use as a directory for e-mails and other contact information.

The GAL provides each user's e-mail address.

The first line, Your Honor, John dot, we'll say, Doe at Iraq at CENTCOM dot mil.

It also provides their user names for their accounts on NIPRNET. John dot Doe, Tasha dot Doe, Sean dot Doe. Their user names to log onto NIPRNET.

You also heard testimony from Chief Royer that the Department of Defense tries to use the same

user names in all e-mails addresses in order to deconflict potential over-redundancies.

Also, Your Honor, individuals' full names, including their unit, office and duty description is included in this information. Christopher specialist 1AAB, an S2 analyst.

Prosecution Exhibits 47, 48, 147, there's going to be a few exhibits here, Your Honor.

Prosecution Exhibits 47 and 48 are the entire listing of the 74,000 entries. One for the names and one for the e-mail addresses. That's PE47 and 48.

Your Honor, Prosecution Exhibits 147 and 148 are the 20-page extracts the witnesses referenced on the stand. A are the unredacted forms and the Bravos are the ones you're looking at right here, Your Honor.

This information is the entire compromised Global Address List as PFC Manning had access and the extracts used by those witnesses that I just explained.

The first portion of an e-mail address is

that individual's user name and as I mentioned a moment ago, Your Honor, this portion not only does it have their name, but their rank, their office and their, potentially their location of where they're working.

Your Honor, according to Chief Royer, in many cases the user names continue for that deconfliction. Knowing user names makes the listed individuals more vulnerable to attack. The information provides adversaries a likely list of longstanding e-mails and (inaudible).

Moreover, Your Honor, in the hands of an adversary intelligence organization, the list is a virtual directory of persons with security clearances as you just saw and intel analysts or sensitivity positions as well as potential map for the unit structure.

In short, Your Honor, the GAL becomes a phone book for exploitation. The release of this list would render the information and potentially the physical security for everyone on the list vulnerable to exploitation and ultimately compromise the

effectiveness of the countless missions that those soldiers are working.

Chief Royer testified that the GAL would be one of the top records that he would seek as op 4.

So according to Sergeant Bigelow, PFC Manning left the S2 shop on 8 May 2010 and started working in the supply room around 9 May 2010.

PFC Manning was upset at the move but most thought it was entirely because of the fight he had with his fellow soldier, but he was actually upset because he lost his all-access pass to SIPRNET and his security clearance which he needed to keep in order to continue compromising classified information.

PFC Manning, however, quickly found something else. Something that he could do to maintain relevance in the fast moving disclosure world and that was based off the WikiLeaks 2008. PFC Manning quickly set about refocusing his energies on NIPRNET and created a tester for himself in the process.

This is Prosecution Exhibit 122, Your Honor. A recovered TASK for PFC Manning to exfiltrate

the Global Address List. This TASK mentioned exfiltrate of CIDNE records under purpose. Also organized and (inaudible) PFC Manning creating a TASK to steal the information of CIDNE and for the Global Address List. Acquire and exfiltrate the GAL from the US forces Iraq, Microsoft Outlook, SharePoint exchange server.

Very precise, Your Honor, e-mail the classifies messages from USFI CIDNE event log method, acquire the documents and exact target. Prosecution Exhibit 122.

Your Honor, Special Agent Williamson, forensic examiner testified that he found Google search page results related to the computer programming to extract that information from a GAL.

The first search was for, quote, Global Address List Macro Outlook, end quote, and in return what has been marked as Prosecution Exhibit 144.

THE COURT: What was the name of the search?

MR. FEIN: Your Honor, Global Address List

Macro Outlook, which is also written down in the search field on Prosecution Exhibit 144.

What's clear from looking at the Google search results, Your Honor, is that that search term brings up potential pages in order to figure out how to extract and exfiltrate that information from Outlook because Outlook did not have a function to allow for the e-mails to be pulled out in batch.

The second search was for, quote, VBA, Outlook write text file, VBA, Outlook write text file.

And that returned the search results that are at Prosecution Exhibit 145, PE145.

Your Honor, VBA stands for, as Special Agent Williamson said, Visual Basic. Visual Basic is a program within Microsoft Outlook, or excuse me, Microsoft Office that allows simple programming in order to have the Microsoft Office Tools programs complete automated tasks. And that was another process that PFC Manning researched in order to figure out how, how to get around the limitation within Outlook of

downloading and exfiltrating all the e-mails.

Special Agent Williamson also testified that Visual Basic and macros are the ways you could do that.

Outlook can only save e-mails by user clicking on "save as" and selecting dot txt file type.

Outlook does not have a function to mass export.

Special Agent Williamson also recovered two different types of files related to the Global Address List from Staff Sergeant Bigelow's computers. Those two files, Your Honor, are what are in, from his testimony, Prosecution Exhibits 47 and 48. The names and then the e-mails files.

Although Staff Sergeant Bigelow and Special Agent Williamson testified that this is ample evidence that PFC Manning used that account at the same time on gmail, financial records, reach out to Adrian Lamo and search for WikiLeaks and Julian Assange on the internet.

According to Mr. Johnson, there's evidence

that PFC Manning moved these files, the names and the e-mail text files, to his personal computer. As you heard from Mr. Johnson he found thousands of exchange formatted names and e-mails in unallocated space.

This act was precisely the same process PFC Manning followed each time he found a disclosed classified material. He would use the US Government system to manipulate the data, download the information from the Government system, transfer the data to his personal computer either by CD or in this case because it's unclassified through e-mail and then package it, transmit the information to WikiLeaks and then delete the information.

The information doesn't appear, Your Honor, in the unallocated space of the computer unless PFC Manning took the additional step of deleting it out of his recycle bin or trying to permanently delete it off of the computer.

He took all the same steps with the Global Address List information as he had previously done with each disclosure. Each of these circumstantial pieces

of evidence corroborates the manner, timeline and impetus behind his actions and proven forensically.

You recall that Chief Royer and Nixon testified that the purposes of the US forces Iraq Global Address List was to facilitate official communications.

Nixon testified that user granted permissions to search for e-mail addresses but not mass download them. Microsoft Outlook or NIPRNET computers had a function -- did not have a function to export or download the e-mails (inaudible) even in Iraq who had an e-mail account used and was listed in the Global Address List directory.

Your Honor, we know that PFC Manning's conduct violated AR25-2 by using an information system in a manner other than intended purpose.

PFC Manning downloaded the U.S. Government information from an Army information system to his user account but to another user's account that belonged to a supervisor, Sergeant Bigelow.

PFC Manning did not have permission from

his supervisor to do this, nor did he have permission from the Army or individuals whose private information he took.

He had no additional or legitimate reason for this action.

PFC Manning took the information out of the safe confines that protected the United States Government information system and the network for his own personal desires by e-mailing through his either Gmail account or burning it onto a CD.

The Global Address List information ultimately ended up on his unsecure personal computer on the internet that his -- well on his personal computer connected to the internet.

PFC Manning exposed the sensitive personal information of his brothers and sisters in arms, including all the civilians deployed in Iraq within the 74,000 names.

Exposed all that information to foreign intelligence collection as well as spear phishers and other electronic invasion schemes.

PFC Manning told each Adrian Lamo that after adversaries used spear phishing, he used the word spear phishing, to attack the United States.

PFC Manning noted that the adversaries are not successful typically because they can't penetrate the air gap.

Instead, it was PFC Manning, Your Honor, who penetrated the air gap, meaning the connection between the US Government systems and the rest of the internet. PFC Manning's actions likely exposed the system relied upon by these service members to electronic intrusion as he knew this from his IA training.

Chief Nixon and Chief Royer testified there would be no reason, Your Honor, no reason to download the Global Address List because without access to an exchange server a person couldn't even send an official e-mail. When you have access to the exchange server, you automatically have access to the Global Address List.

The proper (inaudible) is the information

contained the Global Address List. The value of the information established is by the independent pieces of evidence.

Your Honor, the issue here is whether the 74,000 e-mails were more than the statutory limit for the 641 offense.

Chief Nixon testified that dozens of service members worked on creating and entering the information for each user that goes onto the Global Address List.

Every time a new user soldier entered that information, Chief Royer testified they would take at least 10 minutes to create a new account in the Global Address List. For 74,000 e-mails that is 740,000 minutes, or over 12,000 hours or over 51 days straight with no sleep for one soldier to create every Global Address List entry that PFC Manning stole.

Chief Royer testified that soldiers ranking from Specialist to Chief Warrant Officer 4 created Global Address List entries.

In 2010 a soldier at the rank or grade of

E4 rank the Specialist earned approximately $1,800 per month, which also is approximately $11 per hour assuming a 40-hour work week.

At a rate of $11 per hour for 1233 hours it would cost over $145,000 to create the entries for the GAL. Thus, the salary for a Specialist to create each e-mail address and associated information that PFC Manning took when he stole the GAL would well exceed $1,000.

Your Honor, overall the portion of the GAL that PFC Manning took, he stole, consists of 74,000 users. It is clear that -- excuse me, Your Honor, Mr. Lewis testified that the foreign intelligence services of multiple countries actively seek information in the GAL and would pay for the GAL.

Your Honor, for the last time, the United States requests that the Defense relocate to the witness box and I'm going to hand Appellate Exhibit 617 to the court and the accused.

Your Honor, the foreign intelligence services seek information pertaining to specific

individuals and associated organization information as detailed and Classified Reason Number 9.

Mr. Lewis emphasized that a block of information is more valuable to foreign intelligence services. The GAL reveals unit strength and can be associated with other intelligence to increase adversarial understanding of the United States TTPs because the GAL states duty positions and units.

Thus, Mr. Lewis testified that country 5 and their intelligence services would pay over $3,000 on the low end for the records in the GAL as set forth in Classified Reason Number 10.

Your Honor, the United States is -- or I will retrieve Appellate Exhibit 617 from the Court and the witness.

In this case, Your Honor, as PFC Manning took the deliberate actions I previously described to target, extract, and transfer and then hide US Government information, all for the unofficial purpose of transferring this information to WikiLeaks because they asked for it, in doing so, Your Honor, you heard

testimony that PFC Manning deliberately placed all US Government employees and soldiers in Iraq at personal risk by removing their PI from the NIPRNET protected system. This PI, by Army regulation 25-2, is sensitive information that shouldn't be placed on a personal computer.

When PFC Manning extracted the GAL to his personal computer he completed his theft of those records. The GAL was stored on an unclassified system where only unauthorized or where only authorized personnel could access them.

At no time was PFC Manning authorized to house the GAL on his personal laptop.

Mr. Lewis testified that foreign intelligence services will pay for this type of information precisely because its exclusive possession by the United States Government, provides a significant benefit.

Your Honor, at this time the United States recommends we go in one final recess and then finish the closing.

THE COURT: All right.

MR. FEIN: Or keep going, Your Honor.

THE COURT: No. This is a good time to take a 15-minute recess.

I'd like to see counsel in my chambers to talk about the way ahead during that recess.

(Court in recess.)

THE COURT: Court is called to order.

Let the record reflected all parties present when the court last recessed are present.

Before we proceed with the remainder of the Prosecution's closing argument, counsel and I met in chambers over the recess to look at the way ahead.

First of all, we discussed the Court granted three amendments to the charge sheet and the Government has not made those yet so the Government will do that in recess, Xerox copy of the original charge sheet that has the charges at arraignment.

And secondly, in light of the time, what we are going to do is finish the Government's closing argument today.

We'll start at 0930 with the defense closing argument and rebuttal by the Government if they have any.

MR. FEIN: Your Honor, Specification 1 of Charge 2. In total PFC Manning compromised more than 700,000 classified documents to WikiLeaks and unquestionably knew that anything he compromised to WikiLeaks would be released to the public on the Internet. And how did he know that, Your Honor?

THE COURT: Are you doing Specification 1, Charge 1 or Specification 1 of Charge 2?

MR. FEIN: Your Honor, Specification 1 of Charge 2.

How do we know that, that PFC Manning unquestionably knew that anything he compromised to WikiLeaks would be released to the public on the internet?

First, he repeatedly reviewed intelligence reports discussing the WikiLeaks' mission and its operations no later than 1 December 2009. This included the ACIC report, IRR and C3 document, which

all of them explicitly told PFC Manning anything that he provided to WikiLeaks would be released to the public.

Second, his chat to Julian Assange. While committing his reckless disclosures, PFC Manning contemporaneously engaged in online chats with Julian Assange and urged him to release the documents previously provided by him to the ones that were not released.

Third, his constant research of the world reaction when the documents he compromised to WikiLeaks were released to the public.

And, fourth, his chats with Julian Assange where he released his criminal acts. Your Honor, PFC Manning chose to compromise the documents to WikiLeaks because he knew that WikiLeaks would release them on the internet.

So what did PFC Manning cause to be published by the internet?

The Court took judicial notice of the following facts: On 15 March 2010 WikiLeaks released

the ACIC report, an actual intel report measuring the threat caused by WikiLeaks.

On 5 April 2010 WikiLeaks released the Apache video of a military operation.

On 25 July 2010 WikiLeaks released more than 75,000 SIGACTS from the CIDNE-A database.

THE COURT: What was the date of that?

MR. FEIN: 25 July 2010, Your Honor.

Contained actual tactical reports of significant events occurring in Afghanistan.

On 22 October 2010 WikiLeaks released more than 390,000 SIGACTS from the CIDNE-I database and those containing actual tactical reports of significant events occurring in Iraq.

Your Honor, 27 and 28 November 2010 WikiLeaks began releasing the Department of State cables and that is what the court took judicial notice of and Special Agent Bettencourt testified on 21 August 2011 all the purported cables were released by WikiLeaks and those were actual reports showing how we conduct foreign relations.

Your Honor, 25 April 2011 WikiLeaks receives more than 700 GTMO DABs, detainee assessment briefs, that were actual reports containing intelligence relating to the particular detainees. Each of these records, were produced by United States Government, stored on the SIPRNET, and were integral to the war against terrorism or US foreign policy and diplomacy.

Witnesses testified that the ACIC report, Apache video, SIGACT database, NCD database, SOUTHCOM database, all contained actual and true information thus intelligence. This intelligence was accessible to PFC Manning and PFC Manning made this intelligence accessible to the world on the internet through WikiLeaks.

Your Honor, you have heard evidence that PFC Manning knew he was not authorized to transmit these classified documents to WikiLeaks and WikiLeaks was not authorized to receive classified information. It did not meet the three criteria that PFC Manning knew too well.

You have also heard, well -- an overwhelming amount of evidence that PFC Manning knew that the enemy uses the internet to gather intelligence.

Specification 1 of Charge 2 requires the United States to prove that PFC Manning acted wantonly when he caused this intelligence to be published on the internet, whether all the (inaudible) circumstances his conduct was that he, that a type of heedless nature that made it actually or eminently dangerous to others.

The evidence without question is overwhelming to prove, at the very least is utter recklessness.

PFC Manning compromised more than 700,000 classified documents during the 7-month deployment. That's 100,000 documents per month, 3,300 documents per day, 138 documents per hour and more than two documents every minute.

Your Honor, there is absolutely no way he even knew what he was giving to WikiLeaks as far as the entire large databases. Instead, he learned the exact

details of what he compromised the same time as the public and the enemy.

The individual details, PFC Manning, without question, understood this risk. He told Adrian Lamo that Hillary Clinton and several thousand diplomats around the world were going to have a heart attack when they woke up one morning and found an entire repository of classified foreign policies available in searchable format to the public. He recognized that and even acknowledged that his actions will affect everybody on earth in the same chats.

Lastly, Your Honor, the United States proved that PFC Manning's misconduct was prejudicial to good order discipline and service for all of the Specification of Charge 2.

Colonel Miller, Colonel Miller testified that the last thing he expected was an internal security breach from one of his own, an insider threat from within his ranks.

According to Colonel Miller, when he briefed the staff about PFC Manning's actions, a

funeral-like atmosphere fell over the crowd. They were angry, sad, grieved and frustrated all at the same time.

Colonel Miller testified that before the scope of PFC Manning's misconduct was revealed, the unit morale was at an all-time high. As they had just completed their mission requirements, everything was going well with the Iraqi security forces and they were beginning to do draw-down in order to redeploy to Ft. Drum.

Soldiers that had been on numerous prior deployments within, as he testified, the most deployed brigade in the United States Army, were finally seeing the fruits of their labors over the past 10 years come to fruition.

And then, PFC Manning's covert actions came to light. His misconduct completely shook the entire brigade, according to Colonel Miller. Colonel Miller testified that the morale took a hit. It took a hit as a result of PFC Manning's actions. The unit collectively felt it was a blemish on its otherwise

stellar record.

PFC Manning's recklessness negatively impacted the trusted formation. Colonel Miller testified that trusted information is the foundation for everything we do in the military. Every soldier has to know that every other soldier is doing their job and they have to trust each other in order to stay focused on their mission. Every soldier has to rely on each other and know that they have each other's backs.

Those are the words of Colonel Miller, Your Honor.

If there's a distraction and the soldier has to look to his left and right when he's supposed to be looking in front of him, that his eyes are off his job and the foundation of the military starts to crumble.

Your Honor, according to Colonel Miller, the US Army relies on the trust of (inaudible) PFC Manning's actions caused the morale of the unit to take a hit to create the (inaudible). Thus, Your Honor, it was prejudice (inaudible) and service discrediting.

Your Honor, 104 aiding the enemy by giving intelligence. Your Honor, PFC Manning deliberately transmitted the Apache video, certain Department of State cables information, and the CIDNE-A SIGACTS to WikiLeaks. He did this with the knowledge and intent that it would be released to the world and he did this knowing that the enemy would retrieve this valuable information from WikiLeaks.

Your Honor, for Article 104 purposes, who are the enemies of the United States. You heard evidence from multiple sources, multiple witnesses regarding enemies of the United States and specifically al-Qaeda and al-Qaeda of the Arabian Peninsula.

One of those sources of evidence is your ruling on judicial notice. You took judicial notice that facts establishing (inaudible) and Adam Gadahn are members off al-Qaeda and enemies of the United States, al-Qaeda and Arabian Peninsula are also an enemy of the United States.

Your Honor, you also have Prosecution Exhibit 153. That is a stipulation of fact for Osama

bin Laden.

And you have Prosecution Exhibit 182. The stipulation of fact for Adam Gadahn. You have those for your reference, Your Honor.

Commander Aboul-Enein, through a stipulation of expected testimony, explained the historical background of al-Qaeda and the Arabian Peninsula and how they operate as an enemy of the United States. None of these facts for dispute.

What's specifically contested, but not in dispute, is PFC Manning's knowledge.

PFC Manning had actual knowledge that these enemies,al-Qaeda and al-Qaeda Arabian Peninsula used WikiLeaks to gather intelligence on the United States. And, therefore, by giving intelligence to WikiLeaks he was giving intelligence to the enemy.

PFC Manning had the general evil intent necessary to aid the enemy and evidence shows that he acted voluntarily and deliberately with his disclosures.

The United States proved beyond a

reasonable doubt that PFC Manning's voluntary and deliberate actions to disclose over 700,000 documents to the world and public through WikiLeaks were in the actual hands of the enemy and PFC Manning knew this would occur when he released that information.

The evidence showed that PFC Manning was a trained intelligence analyst. His daily work product as an intelligence analyst in Garrison and in theater established his knowledge of the enemy threat. His research of intelligence reports related to WikiLeaks warned him repeatedly of the enemy's use of WikiLeaks.

In his own statements he established that he knew, he knew through his own words that the information would be made available to the world without alteration.

First, Your Honor, PFC Manning's military training. He was an all-source intelligence analyst at 35 fox. No other MOS in the entire United States Army receive such detail level of instruction on the enemies of the United States, what they're capable of, and why we keep classified information from their possession.

Your Honor, what did PFC Manning learn at AIT about the need to safeguard classified and sensitive information? The dangers of putting such information on the internet and the enemy's use of the internet. He learned the lesson of INFOSEC. Prosecution Exhibit 52. The PowerPoint slide show he received. The lessons on the identity of terrorist groups including al-Qaeda and Osama bin Laden. Lessons on the enemy attempting to discover how and when the US is conducting military operations.

Slide 72 of PE52. 72 of 52.

Lessons not to discuss operational activities on the internet or on e-mail and that soldiers should always assume, always assume, that an adversary is reading posted material on the internet.

Lessons that the enemy used the internet.

Lessons that focused on the enemy piecing together information on the internet to use against the United States includes, PII, unit identification and unit location information.

And, finally, lessons focused on ensuring

information posted on the internet has no significant value to the adversaries because soldiers have to always assume, he was taught, always assume that that adversary is reading their material on the internet.

Your Honor, PFC Manning knew and understood the different types of recruiting utilized by terrorist organizations, in particular al-Qaeda. And the number of terrorist web sites have jumped from less than 100 to as many as 4,000 over the past 10 years.

He also learned about non-disclosure agreements. In 2008 he signed two of them, two non-disclosure agreements accepting responsibility for having knowledge of the potential effects of unauthorized disclosure of classified information. He declared his understanding of being reposed trust and confidence to protect our nation's secrets.

Based on his training and assigning of two non-disclosure agreements, PFC Manning had actual knowledge that terrorist organizations would use WikiLeaks as a source for their intelligence collection.

When disclosing all the classified information from the SIPRNET, PFC Manning understood the consequences of his actions and knew, without any doubt, Your Honor, that the information he compromised would be in the hands of the enemy.

Prosecution Exhibit 25 is a copy of the OPSEC PowerPoint brief he created and taught others.

Prosecution Exhibit 25, his own words, Your Honor.

And, Your Honor, the fact that Osama bin Laden asked for the disclosed information and received it proves that PFC Manning was correct when he taught in Prosecution Exhibit 25 that adversaries, including foreign governments, terrorists and activists and hackers, that's who they are, that the common OPSEC leaks include leaks on the internet and that disclosure of the information on the internet must be avoided because one must use common sense because there are many enemies and it's a free and open society.

Your Honor, that was just, just his knowledge before arriving to 210 Mountain; but what

about PFC Manning, what did he know based on the actual analytic work product that he was required to perform?

He had extensive experience studying enemy TTP, both pre-deployment and during his deployment.

At Ft. Drum he conducted weekly briefings to his superiors on worldwide threats and specific threats in Afghanistan and Iraq.

He was very good at computers. One of his strengths was data mining.

Data mining was critical to the enemy predictive analysis that you've heard about, that study of an enemy trend to be able to predict their future activities.

Mr. Hall testified as an expert, said that PFC Manning would have been aware, he would have been aware that the enemy engaged in similar pattern analysis about the US TTPs and movements.

PFC Manning acknowledges his own understanding of the value of the information that he passed to WikiLeaks by claiming the SigActs for Iraq and Afghanistan are, "possibly one of the most --" or

excuse me -- "one of the more significant documents of our time. Removing the fog of war and revealing the true nature of 21st century asymmetric warfare."

Prosecution Exhibit 42.

Your Honor, in addition to his training and work product, PFC Manning kept different military publications on external hard drive that showed he was not naive or an ignorant soldier but one who methodically kept track of information, including the information regarding the use as weapons of pro-insurgent web sites by the enemy.

The methodology the enemy uses on the internet to further the anti-US causes, including cyber mining for intelligence. Information warfare in the form of propaganda is a well-known enemy tactic.

His possession of all the above data information is additional circumstantial evidence that PFC Manning had actual knowledge leading to the only reasonable inference that he knew by disclosing this information to WikiLeaks, an organization he knew would release any information he was providing them to the

public. He was giving the information to the enemy and specifically al-Qaeda and the al-Qaeda at the Arabian Peninsula.

PFC Manning's knowledge of the enemy using the internet was further developed, Your Honor, in his own searching for repeated reading and habitual compromising of the classified information pertaining to WikiLeaks website.

He read three different intellectual reports that explicitly told him that the enemy will read anything posted on WikiLeaks.

First, Your Honor, the ACIC report. As I already discussed, PFC Manning first accessed this basic website on 19 November 2009 and then viewed the document, the document being Prosecution Exhibit 45 and 46, on 1 December 2009.

So what did PFC Manning learn from that document? That WikiLeaks represented a potential force protection, counterintelligence, OPSEC and INFOSEC threat.

Unauthorized release of classified

documents provide foreign intelligence services and terrorist groups potential actual information against the United States.

That they post all the information they receive without editorial oversight.

That a reader must presume, they must presume foreign adversaries will read and assess any information.

PFC Manning also appreciated the value of the ACIC document in cyber intelligence reporting.

On 15 March 2010 PFC Manning sent an e-mail to Captain Lim and Captain Martin and Chief Balonek and others in the S2 shop stating, quote, occasionally has good hits from extremist website in ROE founded earlier this morning, end quote.

And then to provide the ACIC website in his e-mail, http colon slash slash ACIC portal dot north slash inscom dot Army dot smil dot mil. This e-mail is contained on PE12, PFC Manning's dot 22 SIPRNET computer. PFC Manning read this document on five occasions and he also compromised this document to

WikiLeaks.

Second, Your Honor, NCIRR. As I already discussed. PFC Manning first PE99 after conducting a search for WikiLeaks on Intelink on 1 December 2009. On 14 February 2010 he downloaded the report and disclosed it to WikiLeaks.

So what did he learn from this IRR. That WikiLeaks self-described uncensorable Wikipedia for untracable mass document leading and analysis.

WikiLeaks in 2008 had garnered the attention of major news media outlets but not intelligence reporting within the United States because it was largely north.

Interesting enough, Your Honor, the IRR also included contact information for the NCIS cyber security office.

If PFC Manning had any questions about the threat WikiLeaks posed to our National Security he could have reached out for clarification which he clearly did not do.

However, Your Honor, we do know what he

did, he kept Julian Assange's contact information and he reached out to them in November of 2009 instead of seeking clarification if he actually doubted what he read.

Third, Your Honor, the C3 trip report. As I already discussed, PFC Manning's first would have viewed the C3 report, Prosecution Exhibit 43, after conducting a search for WikiLeaks on Intelink or after January 2010. On 14 February 2010 he downloaded the report and disclosed it to WikiLeaks.

So what did he learn from the C3 report, Your Honor? On page 2, quote, the internet is an essential communication tool for terrorists, end quote. That WikiLeaks is a publicly accessible internet website where individuals submit leaked information and have it published to the public anonymously without fear of being held legally liable.

Information that can be disclosed includes, but not limited, classified information and then on page 3, Your Honor, on page 3 of the C3 report, WikiLeaks poses a large threat not only from the actual

external disclosure, but from the insider, the insider would be able to easily leak information without fear of any direct individual repercussions.

PFC Manning read these three different reports on multiple occasions during his deployment and he chose to compromise those reports.

By reading and disclosing these three documents he knew at a minimum that WikiLeaks had a self-admitted reputation for encouraging leaks of classified information for the United States Government and releasing that information.

By reading and disclosing these three documents PFC Manning knew at a minimum that any website that posts anything it received would be used by the enemy.

These documents, coupled with his intelligence training on the means and methods that al-Qaeda and the Arabian Peninsula employ, PFC Manning knew the exact type of information he chose to disclose would be useful to the enemy.

PFC Manning knew the informations existence

on the internet would actively encourage our nation's enemy to gather and data mine the information just like he had to do for his country as an intelligence analyst.

This is particularly true, Your Honor, in light of PFC Manning's specific training on al-Qaeda at ART, 210 Mountain, JRTC rotations and in-theater.

His own words informed his actual knowledge, Your Honor, deliberate acts of disclosure to WikiLeaks would inevitably result in our nation's enemy possessing the compromised materials. His own statements document knowledge. By giving the information to WikiLeaks (inaudible), PFC Manning knew the information had a global scope and he was creating worldwide anarchy and that was a beautiful and horrifying thing to him. Global scope worldwide anarchy and that was a beautiful and horrifying thing.

That's page 9, Your Honor, of the Lamo chats.

These are not the words of a humanist, but these are the words of an anarchist.

PFC Manning knew how WikiLeaks held themselves out to the world, quote, like you're the first intelligence agency for the general public, end quote. Page 9, Assange chats.

On page 10 of the Assange chats, Julian Assange specifically states to PFC Manning that, quote, WikiLeaks described itself as the first intelligence agency of the people. Better principle and less parochial than any Government intelligence agencies. It is able to be more accurate and relevant. It has no commercial or national interests at heart. It is only interested in the revelation of the truth. Unlike the covert activities at state intelligence agencies, WikiLeaks relies upon the power of overt fact.

Your Honor, PFC Manning's work with an intelligence agency of the people is not an act of a person trying to spark a national debate but rather an act of a soldier, a soldier of the United States Army that has no longer loyalty to his country because he had no, no national interest at heart.

PFC Manning depended on WikiLeaks posting

whatever he disclosed to them on the internet.

Additionally, PFC Manning's chats with Adrian Lamo informed his knowledge of WikiLeaks and the effects of his actions.

He called WikiLeaks a group of FOI activists, he knew the compromise of Department of State cables would affect everybody on earth.

He noted, again, Your Honor, that Hillary Clinton and several thousand diplomats around the world are going to have a heart attack when they wake up one morning and find an entire repository of classified foreign policies available and in searchable format for the public.

He created the searchable format for the public, the public included the enemy and he knew that, Your Honor, as an intelligence analyst.

He even acknowledged that, quote, could have sold the information to Russia and China but chose not to because it's public data. And because another state would take advantage of the information and try to get some edge.

This isn't public data, Your Honor. This is United States Government classified information he was trained to use to protect our soldiers and knew the effects of his actions.

Your Honor, this simple acknowledgement by PFC Manning shows that he understood the utility and financial value of this information and how foreign entities desired the information.

Your Honor, the defense would like you to believe that PFC Manning actually wanted to spark change and reform. However, PFC Manning never once mentioned protecting the American public or the United States as being any sort of motivation for his crimes in any of his chats or e-mails.

Simply put, if PFC Manning had given the information to Russia or China, he would have made an incredible amount of money according to him. If nothing else, he was skilled in constructing post justifications to his acts that were not based in facts, actual actions themselves, the actions that we're discussing here. This is true for the evidence

defense elicited in the McNamara chats and Lamo chats. Based on his actions, Your Honor, admissions to Assange and Lamo, his predeployment admission to Ms. Showman, PFC Manning had no allegiance to the United States and the flag it stands for.

You heard the testimony from Ms. Showman that during a predeployment counseling session she pointed to the American flag on her shoulder and asked PFC Manning what that flag meant to him.

His answer, that flag meant nothing to him. He had no allegiance to any people. Similar words to one who is an anarchist.

Ms. Showman testified that after this incident she notified Sergeant Mitchell and Master Sergeant Adkins.

And, Your Honor, you heard, although suffering from memory problems, that Master Sergeant Adkins testified that he remembered signing his administrative reduction board appeal, that document which occurred two years ago, and on that appeal he recalled Ms. Showman telling him about the incident and

him reporting that incident to Major Clawson, his boss at the time.

PFC Manning did have a general evil intent, Your Honor, which was manifested through his deliberate and repeated compromise of classified information. His wholesale disclosure of information from databases that he could not have even read all the information then. Based on the general evil intent PFC Manning knowingly gave through WikiLeaks al-Qaeda and the al-Qaeda Arabian Peninsula specific intelligence which was found in their possession.

Your Honor, there's no dispute that information from the CIDNE-A database, specifically the SIGACTS, certain Department of State cables and the Apache video are intelligence. And that intelligence was received by al-Qaeda and the al-Qaeda in the Arabian Peninsula.

As the Court is aware, intelligence means any information which is helpful to the enemy and true, at least in part.

First, Your Honor, the CIDNE-A SIGACTS,

Your Honor, according to stipulation of fact for Osama bin Laden on 2 May the United States Government officials raided UBL's compound located in Pakistan and collected several items of digital media. On that media was first a letter from UBL to a member of al-Qaeda requesting that member gather Department of State cables posted to WikiLeaks.

And then also a letter from the same member of al-Qaeda to UBL attached to which were the SIGACTS from the CIDNE-A database as posted by WikiLeaks.

The classified version of the stipulation of fact, Your Honor, Prosecution Exhibit 153 Bravo, 153 Bravo explains exactly what Osama bin Laden asked for and what he exactly received.

Second, Your Honor, the Apache video in a video released about al-Assad media organization operated by al-Qaeda. Adam Gadahn showed the edited version of the Apache video which PFC Manning disclosed to WikiLeaks.

The stipulation of fact for Adam Gadahn, Prosecution Exhibit 182, explains the terrorist video

in which excerpts of the WikiLeaks Apache video weren't present.

Third, Your Honor, Department of State information was in the hands of two different enemies of the United States: Osama bin Laden and Adam Gadahn.

According to the stipulation of fact for Osama bin Laden, Prosecution Exhibit 153, during the raid of his compound United States Government officials also collected Department of State cables information released by PFC Manning.

Your Honor, the classified Department of State cables found in UBL's possession is in Prosecution Exhibit 173 Charlie. And this document makes it clear that in the year of its publication, the intelligence community understood certain capabilities of the enemy and PFC Manning himself ignored those indicators when deciding to compromise all the classification.

Prosecution Exhibit 173 Charlie, in the same terrorist recruitment video released by al-Assad and Adam Gadahn also showed the Department of State

cables information contained from PFC Manning and WikiLeaks.

Prosecution Exhibit 174 Bravo and Charlie described in-depth the Department of State cables information present in the Gadahn video.

In order, Your Honor, for the intelligence 104 article, the purpose of the information must be helpful or useful to the enemy. How is this material helpful to the enemy?

CIDNE-A, Your Honor, you heard testimony that CIDNE-A contains tactical information about how we fight our wars and our enemy inflict damage on our soldiers.

This is our playback, a snapshot unit, TTP, battle drills and call signs. With this information the enemy now knows how each individual unit, company to division, who deploy to Iraq or Afghanistan between 2004 and 2009 executes its wartime mission.

United States faces enemies worldwide and not just in Iraq and Afghanistan. IEDs are not unique to those theaters. Now PFC Manning provided any enemy

of the United States worldwide this data.

The SIGACTS from CIDNE-A details whether the enemy was successful in the attacks against US forces, if a specific IED did or did not work.

The enemy can now use the factual information from the reports to develop their own TTP to better employ IEDs against the United States.

This is the exact same process, Your Honor, that PFC Manning was trained and used when he determined the safest route or the highest density of IED's for his commander.

You heard from Commander Aboul-Enein that acknowledgement of successful attacks against US forces boosts the morale within al-Qaeda and may lead to increase in attacks. This, too, Your Honor, applies worldwide. There is no question why UBL himself wanted this material based on that type of information and he received it.

The Apache video. Your Honor, you heard testimony from Commander Aboul-Enein that media perception is important to al-Qaeda and any event that

places al-Qaeda in a positive light or US forces in negative light is beneficial to al-Qaeda.

The edited and released version of the Apache video is obviously a video that al-Qaeda can use in propaganda.

Terrorist organizations now have it, proven by Adam Gadahn calling on all Jihadists to view the video and war against United States.

PFC Manning knew this would happen from his training when he taught, when he was taught, excuse me, Your Honor, that within the last 10 years the number of terrorists web sites have jumped from 100 to as many as 4,000 and in recruitment.

PFC Manning (inaudible). Department of State cables, you heard testimony from Commander Aboul-Enein that events that undermine the foreign leaders, excuse me, cooperation with foreign leaders, Your Honor, would create an environment, an environment which terrorists, ideology excels through al-Qaeda.

The Department of State cables captures candid discussions with foreign leaders and has a

potential to create the type of hostile environment.

Even PFC Manning himself recognized this in his chat with Adrian Lamo when he stated that line about Hillary Clinton and the several thousand diplomats.

This was even obvious to Osama bin Laden, who wanted this material and he received it, and he received it, asked for this type of material and received it, and he was in the most isolated regions within Pakistan, Your Honor.

PFC Manning also understood the enemy's ability to data mine for information.

As Mr. Hall testified, all junior analysts know that enemy conducts particular analysis based on data it can access and the enemy does this through data mining.

PFC Manning knew this when he decided to make the information available to the enemy in the format he made it available.

Your Honor, Inspire magazine, a magazine published on the internet by al-Qaeda in the Arabian

Peninsula. Inspire magazine serves as a propaganda tool.

On 16 January 2010, Inspire magazine published Issue No. 4, Winter 2010 edition on the internet. On pages 44 and 45 of that issue, the magazine lists activities in western Jihadist to wage Jihad against the United States and the west.

Specifically, the magazine pointed out that archiving large amounts of information is helpful to AQAP and it further lists, "anything useful from WikiLeaks is useful for archiving."

Al-Qaeda in the Arabian Peninsula recognized the value that PFC Manning made available to them through WikiLeaks and directed its followers to perform essentially the same function that PFC Manning did for the United States, data mine for information they could use.

Your Honor, the CIDNE-A SIGACTS, Department of State cables information, the Apache video are all information that is of value to the enemy and thus intelligence.

PFC Manning knew who the enemy was and what type of information they sought, specifically classified information and tactical information.

He knew that the enemy used the internet and that WikiLeaks was helpful to our enemies.

He knew that WikiLeaks website commonly contained classified official US Government information and for that reason was commonly visited by the enemy like any other website like that.

PFC Manning was well-informed of how WikiLeaks operated. He searched for WikiLeaks more than 100 times on Intelink during his deployment or, as you heard earlier, roughly four searches for every five days in theater.

He knew that anything that he disclosed to WikiLeaks would be posted on the internet and he knew that foreign adversaries will review and access DoD sensitive or classified information posted to the WikiLeaks website.

PFC Manning posed that question, Your Honor, to Adrian Lamo in his chats: If you had

unprecedented access to classified networks 14 hours a day, 7 days a week for 8 plus months what would you do?

PFC Manning asked that question six months after he starting exfiltrating information from the SIPRNET. He asked that question six months after he knowingly provided intelligence leaks about the United States through WikiLeaks. (inaudible). He asked that question six months after researching WikiLeaks on Intelink and other classified databases and watching the effects of previous disclosures yet continuing to disclose.

PFC Manning provided his answer to Adrian Lamo on page 8, Your Honor, of his chat: "Let's just say someone I know intimately well has been penetrating US classified networks, mining data like the ones described, and then transferring that data from the classified networks over the air gap onto a commercial network computer, sorting the data, compressing, encrypting it, and uploading it to a crazy white haired aussie who can't seem to stay in one country very long."

What you did not see, Your Honor, in those chats with Julian Assange or Lauren McNamara is that he had a duty to his country and a specific duty to protect classified information and other sensitive information and with this access that he work hard to assist his fellow soldiers that are in enemy sites.

PFC Manning never took pause when divulging to Adrian Lamo that he had created a massive mess and no one, his own words, Your Honor, no one had a clue because 95 percent of the efforts are on physical security of classified networks and managing operational security on unclassified networks.

That's on Lamo page 8 of his charts.

PFC Manning was an anarchist whose agenda was made abundantly clear almost immediately after he deployed to Iraq. He was not naive.

Each time he downloaded and transmitted closely-held information he made deliberate decisions to break ranks with his nation throwing all his training and experience aside and releasing that information to the world.

He used his access to classified networks that Julian Assange claimed held the alleged covert activities of state intelligence agencies and made those secrets overt fact for the world to view, all the while knowing the world included progressive and technologically savvy enemies that used any US Government information against our nation.

Your Honor, in the Assange chats, page 5, page 5, PFC Manning boasts on his knowledge that, "the more the Government controls information, the harder the Government tries, the more violently the information wants to get out."

Your Honor, the information did not just ooze from the SIPRNET onto the World Wide Web for the enemy to access, but was the precise outcome that PFC Manning desired when he took the deliberate steps to disclose over 700,000 documents by moving that information one disk at a time from SIPRNET to his personal Mac bridging that air gap.

Your Honor, rather than focusing on his war fighting mission, he made the decision to disclose the

700,000 from SIPRNET knowing that once WikiLeaks received the information they would release it for the world to access and he knew the world included the enemies of the United States.

He was not a naive or well0intentioned soldier.

Your Honor, a well-intentioned soldier does not claim that: "The State Department fucked itself. Placed volumes and volumes of information in a single spot with no security."

Lamo chats, Your Honor, page 41.

Or, have a conversation recognizing that the only people you trust can fuck you, info-wise at least.

Lamo chats, Your Honor, page 41.

This recognition of system weaknesses and the active and deliberate exploitation of those weaknesses are not the acts of the naive and well-intentioned soldier, but one who acts in a calculated manner and for his own purposes.

The only naivety PFC Manning shows, Your

Honor, throughout his entire endeavor was that despite admitting to his crimes and multiple chats, making admissions of e-mails, keeping trophies of his handy work and not forensically wiping his machine daily, he actually thought he would get away with what he did and he wouldn't get caught.

PFC Manning is a United States Army intelligence analyst that the United States trained and trusted to use multiple intelligence systems to provide real time information to leaders on the battlefield and he used that training to defy our trust and indiscriminately and systematically harvested over 700,000 documents from the SIPRNET during a time of war and while deployed in Iraq in support of that war.

Showing no loyalty to this nation, PFC Manning knowingly gave the enemies of the United States unfettered access to these Government documents and we now know today, Your Honor, as part of this court martial that at least two enemies, at least two enemies received the information; including Osama bin Laden, who at the time of his death was the most isolated and

wanted enemy of the United States, and al-Qaeda in the Arabian Peninsula.

Your Honor, the United States is confident that after reviewing all of the evidence, applying your own common sense knowledge of human nature and the ways of the world and specifically spending time focused on PFC Manning's own words in his chats that you will find him guilty beyond a reasonable doubt of all the charges and their specifications.

Your Honor, PFC Manning was not a humanist; he was a hacker. A hacker who described his fellow soldiers as dikes, a bunch of hyper-masculine, trigger-happy, ignorant, rednecks or gullable idiots.

Lamo chats, Your Honor, page 7 and 37, 7 and 37. Assange chats, page 8.

Your Honor, he was not a troubled young sole. He was a determined soldier with a knowledge, ability, and desire to harm the United States in its war effort. And, Your Honor, he was not a whistleblower; he was a traitor. A traitor who understood the value of compromised information in the

hands of the enemy and took deliberate steps to ensure they, along with the world, received all of it.

Thank you, Your Honor.

THE COURT: All right. Is there anything we need to address before we recess until 09:30?

MR. COOMBS: No, Your Honor.

MR. FEIN: No, Your Honor.

THE COURT: Court is in recess.

(Court recessed at 5:45 p.m.)

$

$1,000 (2)
95:19;122:9
$1,500 (1)
69:14
$1,800 (1)
122:1
$1.3 (1)
25:11
$1.8 (1)
96:11
$1.9 (1)
26:19
$10,000 (2)
24:20;26:8
$11 (2)
122:2,4
$145,000 (1)
122:5
$2,000 (1)
96:7
$3,000 (1)
123:10
$3,850,000 (1)
26:21
$50 (4)
25:4,14;26:12,21
$525,000 (1)
70:1
$7,000 (1)
70:18
$9 (1)
69:17
$9.39 (1)
70:3

A

ability (4)
2:8;30:11;158:12;166:18
able (9)
14:1;17:1;19:10;65:18, 20;87:21;140:12;146:2; 148:10
Aboul-Enein (4)
135:5;156:12,20;157:16
above (1)
141:16
above-titled (1)
1:15
absolutely (1)
130:19
abundantly (1)
162:15
abusing (1)
53:6
acceptable (1)
38:19
accepting (1)
138:12
access (38)
10:6;21:12;33:5;42:11; 45:17;46:12;48:19;49:3; 50:3,9;52:5,14;53:6;56:20; 58:3,5,14;67:18;80:10;82:5, 8,18;83:6;94:8;102:20; 111:19;120:16,18,19; 124:11;158:15;160:17; 161:1;162:5;163:1,15; 164:3;165:17
accessed (12)
32:6,14,19;33:9;34:10; 62:2;73:8;76:6;83:15; 89:15,16;142:13
accessible (5)
83:5;86:14;129:12,14; 145:14
accessing (1)
102:10
accomplish (6)
11:14;80:17;81:10;83:21; 88:8;102:16
accomplishments (1)
20:10
according (19)
63:18;72:12;73:10;74:7, 11;75:17;96:9;101:3; 106:19;110:2;112:5;113:5; 116:21;131:20;132:18; 133:17;150:17;153:1;154:6
accordingly (3)
41:3;68:15;78:2
account (22)
44:3;48:7,9,11,13,16,20; 49:4;53:4,4,9,13;56:9; 57:10;58:9;85:10;116:17; 118:12,19,19;119:10; 121:13
accounts (3)
47:8;109:14;110:18
accurate (2)
2:9;148:10
ACCUSED (10)
3:10;31:3;34:9;45:19; 57:12;70:7;72:8;76:8;95:6; 122:19
accused's (3)
30:21;36:18;74:9
achieve (1)
38:4
ACIC (27)
27:2,14,18;28:1,16;29:3, 21;31:6,18;32:4,9,12,15,15, 19;33:8,10,13,14;34:2; 126:21;128:1;129:9; 142:12;143:10,16,17
acknowledged (2)
131:10;149:17
acknowledgement (2)
150:5;156:13
acknowledges (1)
140:18
Acquire (2)
114:5,10
across (2)
80:11;106:13
act (3)
117:5;148:16,18
acted (2)
130:6;135:19
acting (1)
80:1
action (4)
20:3;34:3;89:19;119:5
actionable (2)
29:16;30:12
actions (23)
19:10;28:21;33:19;34:14; 35:16;40:18;42:6;77:6; 118:2;120:10;123:17; 131:10,21;132:16,20; 133:19;136:2;139:3;149:4; 150:4,20,20;151:2
active (1)
164:17
actively (6)
24:5;25:20;70:12;95:11; 122:14;147:1
activist (1)
35:5
activists (4)
38:4;79:1;139:14;149:6
activities (9)
4:21;74:21;75:2;108:2; 137:13;140:13;148:13; 159:6;163:3
activity (6)
4:20;9:14;13:2;46:4; 47:14;62:18
acts (5)
127:14;147:9;150:19; 164:18,19
actual (24)
2:4;28:2;43:20;48:12,18; 49:9,10;63:4;68:7;128:1,9, 13,20;129:3,11;135:12; 136:4;138:18;140:1; 141:18;143:2;145:21; 147:8;150:20
actually (16)
12:16;36:19;37:12;41:13; 50:3;52:2,20;84:11;88:21; 100:12;101:8;113:10; 130:10;145:3;150:10;165:5
Adam (7)
134:16;135:3;153:17,20; 154:5,21;157:7
add (3)
96:21;99:3,17
addition (1)
141:5
additional (3)
117:16;119:4;141:17
additionally (3)
70:4;100:16;149:2
address (31)
32:14,19;63:5,13;85:21; **108:7;109:12,15,17;110:4, 14;111:19,21;114:1,5,17, 21;116:10;117:20;118:5, 13;119:11;120:16,19;121:1, 10,14,17,20;122:7;167:5**
addressed (2)
28:10;37:1
addresses (6)
32:19;108:19,21;111:1, 11;118:8
adjust (1)
8:1
Adkins (2)
151:15,18
administrative (2)
50:5;151:19
administratively (1)
82:15
administrator (3)
32:13;50:2;99:4
administrators (1)
99:3
Admiral (4)
23:8;61:4,9;107:16
admission (1)
151:3
admissions (2)
151:2;165:3
admitted (5)
13:18;18:2;21:3;69:7; 100:11
admitting (1)
165:2
Adrian (12)
14:3;20:20;59:20;84:14; 116:18;120:1;131:4;149:3; 158:3;160:21;161:12;162:8
advance (1)
38:5
advanced (1)
11:20
advantage (2)
76:10;149:20
adversarial (1)
123:7
adversaries (12)
23:5,7;29:16;30:7;36:12; 112:9;120:2,4;138:2; 139:13;143:7;160:17
adversaries' (1)
30:10
adversary (3)
112:12;137:15;138:4
advise (1)
80:19
affect (3)
77:5;131:11;149:7
afford (1)
87:4
AFG (1)
14:10
Afghanis (1)
19:20

Afghanistan (24)
4:7;9:2,12;10:9,15;11:19;
12:2,3,7,8,10,12,21;14:16;
19:21;24:7,13;29:5;103:11;
128:10;140:7,21;155:17,20
again (13)
4:4;13:1;19:7;48:3;59:5;
63:5;71:21;74:13;79:12;
84:19;85:11;89:8;149:8
against (12)
10:4;28:4;30:14;129:7;
137:18;143:2;156:3,7,13;
157:8;159:7;163:7
agencies (3)
148:9,13;163:3
agency (4)
71:9;148:3,8,16
agenda (2)
42:9;162:14
Agent (60)
12:19;13:16,19;14:14,21;
17:1;32:2;48:8;49:6,14;
50:13,20;51:4,7;52:1,4;
53:7;54:5,14,16;55:14;
56:21;58:4;62:11,14;63:6,
10;64:1,5,16,21;65:8;72:12,
17;73:4,19;79:8;83:4,17;
84:21;85:9,12,20;87:14,16;
88:14,21;89:6,9;93:14;
101:20;104:2,21;109:7;
114:12;115:15;116:2,9,16;
128:18
ago (3)
43:19;112:2;151:20
agreements (4)
107:5;138:11,12,18
ahead (2)
125:6,13
aid (3)
34:14;87:14;135:18
aiding (1)
134:1
aids (1)
6:5
air (5)
107:21;120:6,8;161:17;
163:19
aircraft (1)
35:14
airstrike (1)
103:9
AIT (2)
37:18;137:2
al-Assad (2)
153:16;154:20
ALEXANDER (1)
3:8
algorithm (5)
46:10;49:14,17;55:1,1
all-access (1)
113:11
alleged (1)
163:2
allegiance (2)
151:4,11
allow (4)
11:5;83:13;98:1;115:7
allowed (5)
83:18;87:8;88:2;96:18,19
allows (3)
82:10;89:7;115:17
all-source (2)
81:11;136:17
all-time (1)
132:6
almost (1)
162:15
alone (1)
83:15
along (4)
5:19;17:17;40:2;167:2
Alpha (9)
15:14,19;31:15,16,21;
74:18,18;75:6;78:15
al-Qaeda (28)
134:13,13,17,18;135:7,
13;137:8;138:7;142:2,2;
146:18;147:6;152:9,9,16,
16;153:6,9,17;156:14,21;
157:1,2,4,19;158:21;
159:12;166:1
alteration (1)
136:15
although (8)
18:7,20;33:9;36:5;37:12;
43:13;116:15;151:16
always (4)
137:14,14;138:3,3
ambassador (1)
77:5
amendments (1)
125:15
America (1)
81:3
American (2)
150:12;151:8
among (1)
69:6
amount (4)
33:16;91:4;130:2;150:17
amounts (1)
159:9
ample (1)
116:16
analysis (6)
6:12;28:16;140:11,17;
144:9;158:14
analyst (12)
28:14;38:20;81:8,11;
106:18;111:6;136:7,8,17;
147:4;149:16;165:8
analysts (7)
5:18;6:1;11:5;60:20;
106:18;112:14;158:13
analytic (1)
140:2
analyze (1)
60:7
analyzes (1)
29:3
anarchist (3)
147:21;151:12;162:14
anarchists (1)
38:4
anarchy (4)
84:14,17;147:15,17
ANGEL (1)
3:6
angles (1)
35:13
angry (1)
132:2
Anica (2)
6:18;7:11
annotate (1)
32:3
annotated (2)
56:11;105:13
announcements (1)
42:3
anonymize (1)
48:20
anonymously (1)
145:16
answered (1)
82:14
anticipated (1)
10:14
anti-government (1)
38:3
anti-US (1)
141:13
AO (1)
10:19
Apache (26)
34:20;35:3,9,10,12;36:6;
39:13,14,18;40:6,10;42:17,
21;105:12,18,20;128:4;
129:10;134:3;152:15;
153:15,18;154:1;156:19;
157:4;159:19
appeal (2)
151:19,20
appear (3)
78:10;106:9;117:14
APPEARANCES (1)
3:1
Appellate (9)
23:18;27:11;70:8;71:15;
72:2;95:7;96:13;122:18;
123:14
applied (1)
18:10
applies (1)
156:15
applying (1)
166:4
appointed (1)
79:15
appreciated (1)
143:9
appropriate (1)
38:19
approval (1)
97:2
approve (1)
41:12
approved (1)
53:3
approving (1)
41:10
approximately (7)
25:11;26:19;63:18;69:14,
20;122:1,2
April (17)
29:6;43:2;66:17;75:18,
19;90:6,7;91:8;93:9;104:3;
105:3,7,9,11,12;128:3;
129:1
AQAP (1)
159:10
AR25-2 (8)
52:9;64:19;99:17;100:18;
101:6;109:20;110:2;118:15
Arabian (11)
134:13,18;135:7,13;
142:2;146:18;152:10,17;
158:21;159:12;166:2
archiving (2)
159:9,11
area (4)
7:4,5;81:5;109:5
areas (2)
81:8;95:16
argue (1)
105:5
argued (1)
8:13
arguing (1)
102:10
argument (5)
23:20;71:17;125:12,21;
126:2
arms (1)
119:16
ARMY (23)
1:2,7,9;28:7;29:2,5,12;
69:13;98:1,10,10,11;99:11;
102:16;118:18;119:2;
124:4;132:13;133:18;
136:18;143:18;148:18;
165:7
Army's (1)
53:2
around (5)
72:16;113:7;115:21;
131:6;149:9
arraignment (1)
125:18
arrest (1)
40:9
arriving (1)

139:21
ART (1)
147:7
Arteli (1)
32:12
Article (2)
134:9;155:7
articles (1)
43:9
articulated (1)
74:17
ASHDEN (1)
3:4
Asia (1)
81:3
aside (1)
162:20
ASP (1)
32:7
Assange (35)
33:18,21;34:8;47:19,21;49:5;53:16,19;54:1,12,17;55:11;56:8,12;57:9;58:11;59:17;66:5,7,10,14;69:2;77:1;116:19;127:4,7,13;148:4,5,6;151:2;162:2;163:2,8;166:15
Assange's (1)
145:1
assess (4)
29:1;30:7;42:1;143:7
assessment (2)
60:9;129:2
assessments (3)
28:14;59:12;69:19
assigning (1)
138:17
assist (2)
80:19;162:6
assistance (4)
49:4;53:21;54:8;56:7
assisted (1)
38:11
associated (5)
32:14;39:19;122:7;123:1,6
assume (5)
107:7;137:14,14;138:3,3
Assuming (2)
69:16;122:3
asymmetric (3)
4:13;18:19;141:3
atmosphere (1)
132:1
attached (1)
153:9
attachments (1)
16:19
attack (10)
5:6,8,9,10,11;98:11;112:8;120:3;131:7;149:10
attacking (1)
98:10
attacks (7)
8:2;24:11;26:4;98:17;156:3,13,15
attempt (4)
62:20;63:3,11;65:21
attempted (6)
52:15,20;54:1,8;58:9;62:7
attempting (1)
137:9
attempts (4)
49:3;62:9;63:15,16
attention (6)
33:19;40:13;41:2;43:14;60:4;144:11
attitude (1)
44:5
attributable (1)
48:10
audio (2)
2:7;42:4
audio/video (1)
2:6
audit (1)
47:14
August (2)
92:17;128:19
aunt (2)
15:20;44:1
aunt's (4)
15:1;17:18;19:15;21:15
AUP (1)
64:10
aussie (1)
161:20
authenticity (2)
34:2,5
author (2)
37:14;45:4
authority (5)
31:17;97:6;99:2,21;107:8
authorization (3)
78:12;96:20;97:16
authorize (1)
99:13
authorized (26)
21:11,13;64:10;67:17,19;75:2;94:7,9;96:15;97:12,13,14;98:12;99:8,11,20;100:20;101:6,8,9;102:13,17;124:10,12;129:17,19
authors (2)
52:9;98:21
automated (2)
99:9;115:19
automatically (2)
88:18;120:19
available (18)
7:16;12:11;21:10;22:16;31:7;44:7,10;67:3;80:4;103:16;108:5;109:6;131:9;136:14;149:12;158:18,19;159:13
aviation (1)
36:1
avoided (1)
139:17
aware (3)
140:15,16;152:18
away (3)
19:10;101:18;165:5

B

back (7)
27:6;38:9;41:1;54:3;83:10;90:13;93:18
background (2)
101:21;135:7
backs (1)
133:9
backup (8)
2:7;12:12,14;91:15,16;92:3;93:4,12
bad (1)
49:15
Baghdad (3)
80:20;81:1,6
Balonek (2)
38:16;143:12
banner (3)
78:11;106:13,16
bar (2)
83:7;84:4
Base (2)
1:10;69:15
Base64 (3)
90:18,19;91:12
based (19)
6:15;10:13,14;16:10;25:9;26:17;37:18;44:9;70:2;77:1;96:3;113:17;138:17;140:1;150:19;151:2;152:8;156:17;158:14
basic (5)
30:5;115:15,15;116:3;142:14
basis (2)
6:14;59:10
batch (7)
13:9,12;83:14;89:7,7,10;115:8
battle (1)
155:15
battlefield (2)
18:19;165:10
BE22PAXwmv (1)
103:8
BE22PAXzip (3)
103:16,19;105:2
beautiful (2)
147:15,17
become (1)
8:2
becomes (1)
112:17
becoming (1)
20:5
began (6)
11:1;64:6;76:20;84:18;103:7;128:16
beginning (5)
32:20;33:3;60:1;71:6;132:9
begs (1)
4:17
BEHALF (2)
3:3,10
behind (6)
48:12,15,18,21;92:20;118:2
belonged (1)
118:19
belonging (1)
71:8
beneficial (1)
157:2
benefit (5)
8:7;22:5;68:11;94:21;124:18
benefits (1)
36:12
best (3)
84:6;87:9;100:5
Bettencourt (2)
79:8;128:18
better (3)
66:2;148:8;156:7
beyond (2)
135:21;166:8
Bigelow (3)
113:5;116:15;118:20
Bigelow's (1)
116:11
biggest (2)
41:2;42:15
bin (11)
8:21;117:17;135:1;137:8;139:10;153:2,13;154:5,7;158:6;165:20
black (2)
55:3,16
Blah (4)
73:20;74:4,9,11
B-L-A-H (1)
73:21
blemish (1)
132:21
block (1)
123:3
bloop (2)
92:4,7
board (1)
151:19
boasts (1)
163:9
bold (1)
55:3
book (6)

37:9,11,17;45:2,7;112:18
boosts (1)
156:14
boot (2)
50:14;52:6
bootable (1)
51:1
booting (3)
52:18;57:21;58:6
boss (1)
152:1
Boston (5)
15:8,10;16:14;17:16,20
both (13)
12:6;22:21;23:10;73:16,21;74:20;85:3;91:1;95:7;96:20;98:17;107:12;140:4
bottom (10)
11:12;31:12;54:13,20;55:16;56:6,14;66:21;87:17;106:8
box (3)
23:16;70:8;122:18
bradass87 (1)
75:18
Bradley (3)
1:6;73:13;74:5
bragged (1)
66:13
branch (3)
28:14;61:14;69:9
Bravo (5)
15:14,19;153:12,13;155:3
Bravos (1)
111:16
breach (1)
131:18
breached (2)
53:1;57:12
break (1)
162:19
bridging (1)
163:19
brief (2)
97:5;139:7
briefed (2)
6:14;131:21
briefings (2)
10:13;140:5
Briefs (3)
59:12;60:10;129:3
brigade (3)
100:9;132:13,18
bring (1)
88:6
brings (1)
115:5
broken (1)
46:9
brothers (1)
119:16
brought (1)
43:13
browser (12)
47:10;82:10,14;83:9,10,19;86:14,18,20;88:5;89:15;102:14
built-in (1)
53:1
bulletin (1)
99:21
bunch (2)
38:3;166:12
burned (5)
39:18;43:16;51:11;74:12;92:14
burning (2)
51:21;119:10
button (1)
82:21
bypass (9)
50:7;52:20,20;57:16;58:9;83:21;87:10;88:3;99:8
bypassed (1)
58:1
bypassing (2)
52:10,12
bz2 (1)
13:16

C

C3 (5)
126:21;145:5,7,11,20
cable (20)
40:3;76:21;77:4,15,19;78:11,13,19;82:11,11;83:6,9,9,18;86:18,19,19;89:15;90:17;91:20
cables (68)
34:10;36:21;45:21;76:13,17;77:13,16,21;78:2,9,9,17,17,21;79:4,9,12,16,20;81:13,21;82:6,9,19;83:1,16;84:2,3;86:11;87:5,11;88:1,14;89:3,16,18;90:2,5,9,14;91:9,11;92:18;93:7,8,10,13,19,20;94:12,15;95:1;96:5;102:12;103:1;128:17,19;134:4;149:7;152:14;153:7;154:9,12;155:1,4;157:15,20;159:19
calculated (1)
164:20
call (2)
108:18;155:15
called (19)
4:2;18:2;20:21;25:1;26:10;48:4;49:12,14;51:3;54:14;55:5,8;59:3;70:19;84:11;85:21;90:18;125:8;149:5
calling (1)
157:7
came (4)
18:8;97:20;99:10;132:16
camera (2)
19:16,16
can (22)
6:3;8:1;33:8;50:2;54:18;55:16;58:18;61:19;77:17;82:5,18;83:11;98:15,18;107:14;116:5;123:5;145:18;156:5;157:4;158:15;164:13
candid (1)
157:21
capabilities (2)
52:10;154:15
capable (3)
42:7;97:19;136:20
capacity (1)
98:9
CAPTAIN (21)
3:5,6,7,8,12;6:11,13;9:21;38:15,18;43:14;64:11;80:15,18,21;82:17;83:17;98:6,17;143:12,12
capture (1)
4:21
captured (9)
4:20;5:3,5;7:1,9,10;9:18;13:2;47:14
captures (2)
73:2;157:20
capturing (1)
47:10
card (14)
4:15;13:17,20;14:19,21;15:5,5;17:17;18:1;19:16;20:6,9,12;21:15
carrying (1)
8:2
Carter (2)
80:1;82:4
case (8)
12:15;28:18;37:5;54:4;66:19;110:10;117:10;123:16
cases (1)
112:6
casualties (1)
5:8
casualty (1)
103:13
cataloged (1)
91:19
catenate (1)
89:1
caught (2)
58:16;165:6
cause (8)
23:2,12;31:4;61:5;75:4;79:14;107:14;127:18
caused (4)
105:20;128:2;130:7;133:19
causes (1)
141:13
causing (2)
68:15;95:1
cavalier (1)
44:5
CD (14)
50:14;51:2,5,6,13;52:7,19;57:19;58:6;74:12;92:15;96:19;117:10;119:10
ceased (1)
94:2
Centaur (2)
13:1,7
CENTCOM (13)
9:9;12:5;23:8;44:12;103:12,20;104:8,9,14;105:4;106:11;107:17;110:16
center (1)
75:20
Center's (2)
28:8,10
Centric (1)
95:13
century (3)
4:13;35:10;141:3
certain (6)
5:20;10:3;48:2;134:3;152:14;154:15
chain (1)
88:18
Chamberlain (1)
32:18
chambers (2)
125:5,13
chance (1)
47:14
change (3)
56:18;97:4;150:11
changed (1)
47:9
channels (1)
75:16
characterize (1)
66:15
Charge (39)
4:8;22:9,10,19;23:9;27:17,18;28:16;30:17;34:20;45:10,13;47:1;59:11,12;64:20;71:3,10;74:15;76:15,15;103:4,5;106:3;107:9;108:8,9,9,14;109:14,19;125:15,18;126:5,11,11,13;130:5;131:15
charged (12)
22:18;28:10;34:19;37:2;66:19;71:2;72:3;78:8;79:11;106:6;107:13,20
charges (3)
109:20;125:18;166:8
Charlie (7)
78:7,7,7;79:13;154:13,19;155:3

charts (1)
162:13
chat (13)
33:18;54:12;55:21;56:15;
84:16;99:20;100:3;101:8;
102:1,2;127:4;158:3;
161:13
chats (33)
14:3;21:2;34:8;45:2;
46:9;47:19,21;53:16;55:10;
56:7,11;66:5,10;81:14;
127:6,13;131:11;147:19;
148:4,5;149:2;150:14;
151:1,1;160:21;162:2;
163:8;164:11,15;165:2;
166:7,14,15
chatted (2)
53:18;57:8
chatting (1)
54:17
check (1)
97:1
Cherepko (3)
38:18;98:6,17
Chief (26)
35:8,20;36:11;38:16;
44:11;69:9;96:17,20;98:3,8,
15,17;101:17;102:1;110:6,
20;112:5;113:3;118:3;
120:14,14;121:7,12,18,19;
143:12
China (2)
149:18;150:16
choose (1)
98:18
chooses (1)
98:19
chose (6)
10:6;81:12;127:15;146:6,
19;149:18
Christmas (2)
33:11;106:2
Christopher (1)
111:5
CHU (1)
56:16
CIDNE (25)
4:7;9:2,8;11:4,12,18;
12:2,6,10,20;13:14;20:7;
21:1,7,9,17;22:6;24:6;39:5,
6;43:20;82:21;114:2,4,9
CIDNE-A (23)
4:15;10:9;11:16;12:17;
13:5,12;14:7,20;21:3;
23:11;24:1,21;25:8,11;
128:6;134:4;152:13,21;
153:10;155:10,11;156:2;
159:18
CIDNE-I (12)
4:15;10:7;14:7,20;23:10;
25:16,21;26:8,9,16,19;
128:12
CIDNE-Iraq (2)
4:7;12:8
circumstances (3)
98:11;103:13;130:8
circumstantial (2)
117:21;141:17
circumvent (2)
57:18;88:3
circumventing (1)
50:6
civilian (1)
103:13
civilians (1)
119:17
claim (1)
164:8
claimed (3)
45:3;77:5;163:2
claiming (1)
140:20
clandestined (1)
43:13
clarification (2)
144:19;145:3
Class (4)
6:18;7:11;10:20;11:9
classic (1)
11:12
classification (6)
31:17;91:1;106:8,20;
107:6;154:18
classified (94)
18:8;19:6;21:10;22:1,11,
12;23:11,17,19;24:13,15;
25:2;26:6,11;27:3,20;28:3;
29:6,14,19;30:1,8;31:1,1,
13,16,20;34:4,6,15;36:6;
44:8;53:6;59:15;60:16,18;
61:7,12;64:8;67:17;68:6,19,
21;70:16,20;71:5,16;74:16;
75:16;76:17;78:2;94:6,17;
95:4,16,20;106:4,19;107:3,
7,18;108:5;113:13;117:7;
123:2,12;126:6;129:18,19;
130:15;131:8;136:21;
137:2;138:14;139:1;142:7,
21;145:19;146:10;149:11;
150:2;152:5;153:11;
154:11;160:3,7,18;161:1,9,
15,17;162:4,11;163:1
classifies (1)
114:9
Clawson (1)
152:1
clear (9)
18:10;20:9;33:19;55:19;
86:8;115:3;122:12;154:14;
162:15
clearance (2)
38:20;113:12
clearances (1)
112:13
clearing (2)
48:1,3
clearly (2)
34:7;144:20
click (10)
11:11,15;42:14;62:12,14;
82:21;83:7,8;86:18;87:18
clicking (6)
65:4;83:12;84:4,5;86:15;
116:6
Clinton (3)
131:5;149:9;158:4
close (1)
107:21
closed (1)
72:19
closely (4)
22:16;36:18;48:17;78:4
closely-held (4)
67:6;76:17;109:4;162:18
closing (5)
23:19;124:21;125:12,20;
126:2
clue (1)
162:9
code (7)
63:4,5,7,12,16;64:12;
108:2
coincidence (2)
108:10,16
Collateral (3)
41:6;43:10;105:16
colleagues (2)
38:21;107:1
collect (2)
27:8;62:10
collected (2)
153:4;154:9
collection (3)
30:13;119:20;138:21
collectively (1)
132:21
colloquy (1)
2:17
colon (1)
143:17
Colonel (18)
1:17;6:14,16;22:21;34:1;
67:7;100:2,4;107:12;
131:16,16,20;132:4,18,18;
133:3,10,17
combat (1)
107:21
combinations (1)
2:15
combine (1)
9:11
Combined (1)
9:7
command (4)
65:11;88:19;89:19;
101:19
commander (16)
5:18;6:3,5,11;22:21;23:9;
60:12;99:12;101:9;107:11,
17;135:5;156:11,12,20;
157:15
commanders (5)
5:15;6:9,20;8:15;99:21
commands (1)
89:6
commercial (2)
148:11;161:17
committing (1)
127:5
common (3)
139:15,18;166:5
commonly (2)
160:6,8
communicate (1)
29:8
communicating (2)
36:12;77:21
communication (1)
145:13
communications (1)
118:6
community (3)
36:1;80:9;154:15
Company (2)
1:8;155:16
compared (1)
43:14
competent (1)
107:8
compilation (1)
18:12
compilations (1)
30:11
complete (7)
16:7,9;30:11;62:8;63:8,
13;115:19
completed (5)
21:7;67:15;94:5;124:8;
132:7
completely (3)
22:7;68:12;132:17
complex (1)
88:8
complicated (1)
49:13
compound (2)
153:3;154:8
compressed (1)
91:11
compressing (1)
161:18
compromise (14)
33:14;36:2;68:7;77:9;
84:10;103:21;105:7;
106:12;112:21;127:15;
146:6;149:6;152:5;154:17
compromised (22)
24:21;27:13;35:1;38:9;
60:8;71:8;78:9;79:14;
81:18;93:20;103:8;111:18;
126:5,7,15;127:11;130:14;
131:1;139:4;143:21;

147:11;166:21
compromising (7)
18:8;40:10;61:5;76:20;
103:18;113:13;142:7
computer (95)
12:20;13:5;15:4,12,15;
16:3,13,17;17:3,5,9,12;
20:12;21:7;32:11;39:3,20;
40:1;43:11;47:5;50:7,10,
14;52:6,19;53:3,10,20;56:8;
57:16,21;58:13;64:6,8,14;
65:5,9;67:15;68:21;69:1;
72:10,15,16;73:3,15;74:10;
76:2,3,4;84:20;85:8,15,17;
86:7,10;87:3,17;88:4,7;
89:11;90:4,12,16;91:5,16;
92:12,15;94:4,10;96:16,18;
98:13;99:13;100:13,20;
102:6,7,15,18,19;104:6,13,
15,17;114:14;117:2,10,15,
18;119:12,14;124:6,8;
143:20;161:18
computers (10)
48:6,9;49:1;97:6,12;99:5;
110:3;116:11;118:9;140:8
computer's (2)
49:18,19
conceal (1)
53:5
concern (1)
47:18
concerns (1)
74:21
concludes (1)
30:5
condenses (1)
90:20
conduct (5)
36:19;78:5;118:15;
128:21;130:9
conducted (6)
42:18,20;46:2;55:4;96:1;
140:5
conducting (6)
35:17;77:21;103:12;
137:10;144:3;145:8
conducts (1)
158:14
confidence (1)
138:16
confident (1)
166:3
confidential (1)
79:17
configured (1)
50:15
confined (1)
44:3
confines (1)
119:7
confirmed (1)
34:2
confirming (2)
34:5;56:3
conflicted (1)
20:3
connected (5)
12:20;13:5;90:4,12;
119:14
connecting (2)
43:20;104:18
connection (3)
108:11,17;120:8
connections (1)
90:1
consequences (1)
139:3
conservative (3)
25:1;26:10;70:20
considered (1)
4:17
considering (1)
106:1
consistent (1)
44:4
consisting (1)
106:6
consists (2)
9:14;122:11
constant (2)
10:18;127:10
constituted (2)
96:4;99:7
constructing (1)
150:18
contact (4)
108:21;110:11;144:15;
145:1
contain (5)
2:13;36:21;60:16;76:16;
78:3
contained (27)
11:4;23:1;24:5;25:20;
31:2;32:7;37:8,21;67:12;
70:12;74:17,20;75:7;76:13;
77:19;78:11,18;79:13;
95:11;107:13,20;121:1;
128:9;129:11;143:19;
155:1;160:7
containing (9)
10:8,9;14:8,19;25:4;
26:13;32:15;128:13;129:3
contains (2)
35:21;155:11
contemporaneously (1)
127:6
content (5)
14:2;35:7;37:16,16;50:3
contents (5)
20:13;50:17;52:3;59:16;
78:17
contested (1)
135:10
continue (9)
6:6;24:16;27:9;29:20;
53:5;71:15;109:3;112:6;
113:13
continued (2)
1:16;20:17
continuing (1)
161:10
contractor (1)
97:3
contrary (1)
12:18
contravention (1)
34:3
control (1)
2:8
controls (1)
163:10
conversation (1)
164:12
convert (1)
90:17
converted (4)
21:16;55:5;68:1;94:11
converts (2)
49:11;57:3
conveyed (3)
21:18;68:1;94:12
convoy (2)
5:2;6:7
cool (1)
38:2
COOMBS (2)
3:11;167:6
cooperation (2)
61:3;157:17
copied (5)
20:12;44:18;85:14;89:4;
102:19
copy (11)
23:18;43:16;50:21;51:5;
86:10;88:11,15,15;102:17;
125:17;139:6
correlate (2)
6:20;8:6
corroborates (1)
118:1
cost (2)
69:21;122:5
counsel (2)
125:5,12
counseling (1)
151:7
Counterintelligence (5)
28:8,13;29:1,11;142:19
counterterrorism (1)
70:15
countless (1)
113:1
countries (5)
24:4;25:19;70:11;95:10;
122:14
country (13)
24:20;26:7;34:18;42:12;
70:17;79:2;95:18;96:6;
123:9;147:3;148:19;
161:20;162:3
coupled (1)
146:16
course (2)
58:14;93:15
court (48)
2:2,13;4:2,3,4;6:19;
23:18;27:11;58:21;59:2,3,3,
4,5;61:8;62:4,16;70:9;
71:14,18;72:20;92:5,21;
93:2;95:8;96:13;97:20;
108:13;114:19;122:19;
123:14;125:1,3,7,8,8,10,14;
126:10;127:20;128:7,17;
152:18;165:18;167:4,8,8,9
COURT-MARTIAL (1)
1:6
courtroom (1)
2:4
covering (1)
47:3
covert (3)
132:16;148:13;163:2
cracking (4)
45:10;53:12;56:1,8
craved (2)
40:13;105:21
crazy (1)
161:19
create (14)
12:14;51:1;70:1;79:19;
84:14,16;89:12;121:13,16;
122:5,6;133:20;157:18;
158:1
created (16)
13:20;20:14;54:4,16;
72:17;74:5;80:6;86:4;92:3,
5,10;113:19;121:19;139:7;
149:14;162:8
creating (6)
28:8;69:21;99:7;114:3;
121:8;147:14
creation (1)
69:12
credentials (1)
53:5
credits (1)
41:10
crimes (2)
150:13;165:2
criminal (2)
109:15;127:14
criteria (1)
129:20
critical (2)
7:13;140:10
crowd (1)
132:1
crumble (1)
133:16
CSQ (1)
14:15
CSV (4)

14:9,10,11,12
current (1)
71:4
currently (1)
9:5
cyber (4)
28:13;141:13;143:10;
144:15

D

D6-A (11)
12:15;39:19;48:9;52:19;
53:3;65:5;87:2;97:3,12;
99:18;102:14
DAB (10)
61:14,21;62:2,20;67:8;
69:8,9,10,12,19
DABs (42)
59:12,14;60:9,11,11,16,
21;61:5,5,11,14,18;62:10,
12;63:15;65:15,17;66:4,8,9,
12,15,18,19,21;67:1,3,14,
16;68:1,4,6,12,16;69:21;
70:1,3,4,12,13;84:7;129:2
daily (2)
136:7;165:4
damage (3)
31:5;61:6;155:12
dangerous (1)
130:10
dangers (2)
30:19;137:3
dat (3)
73:2,6;104:12
data (29)
8:12,14,14;9:7;13:2;
30:11;52:21;63:3,10;72:14;
92:12;96:2;98:18;117:8,9;
140:9,10;141:16;147:2;
149:19;150:1;156:1;
158:12,15,15;159:16;
161:15,16,18
database (50)
9:2;10:8,9;11:13,19;12:2,
10;13:10,12;21:4,7;24:1,21;
25:8,11,16,21;26:9,16,19;
59:18;62:7;65:15,16,19;
70:13,19;76:13,16;77:9,10;
78:10;82:3,6;86:13;87:7;
88:1,12;95:13,20;96:10;
102:11,12;128:6,12;129:10,
10,11;152:13;153:10
databases (16)
11:3,4,16;13:14;14:8,20;
20:18;21:1,9,17;22:6;39:5,
6;130:21;152:6;161:9
dataset (4)
4:6;59:7;76:12;103:3
datasets (1)
23:10
date (5)
6:19;16:13;46:14;62:4;
128:7
dated (2)
72:4;93:7
dates (3)
72:4;75:11;79:10
DAVID (3)
3:11;61:4,9
Davis (1)
67:8
day (13)
5:16;6:9;9:5;41:1;56:18;
74:3;81:17;92:15;105:3;
108:11,17;130:17;161:2
days (13)
13:7,12;14:17;19:1,2;
33:5;43:1,16;83:1;90:9;
121:15;160:14;161:2
DC (1)
77:18
dealing (1)
10:12
death (2)
79:2;165:21
debate (1)
148:17
decades (3)
76:17;79:10;81:12
December (13)
10:21;32:10,16,16;33:9;
38:9,14;46:5;62:1,5;
126:20;142:16;144:4
decide (5)
6:6,16;34:17;86:20;105:8
decided (4)
38:3;50:7;86:18;158:17
deciding (1)
154:17
decision (1)
163:21
decision-making (1)
8:15
decisions (5)
5:16;6:10;8:5,16;162:18
declared (1)
138:15
declassified (1)
27:19
deconflict (1)
111:2
deconfliction (1)
112:7
decrypting (1)
53:12
default (1)
47:9
defeat (3)
5:12;6:10;8:5
defense (24)
8:13;12:13,16;16:15,15;
20:3;22:20;31:19;34:12;
36:15;67:8,10;70:9;74:17;
75:4;80:3;95:8;96:13;
107:10;110:21;122:17;
126:1;150:9;151:1
defense's (1)
67:7
definition (1)
4:19
defy (1)
165:11
delete (2)
117:12,17
deleted (2)
16:12;109:13
deleting (1)
117:16
deliberate (11)
45:1;54:6;57:18;123:17;
136:2;147:9;152:4;162:18;
163:16;164:17;167:1
deliberately (6)
10:6;28:5;45:6;124:1;
134:2;135:19
delivered (1)
69:3
demander (1)
61:10
demonstrate (1)
61:1
demonstrative (1)
87:14
Denise (1)
1:18
density (1)
156:10
denying (1)
34:5
Department (31)
77:12,16,17;78:16;79:18;
80:2,3,9;82:7;84:13;87:11,
21;90:1,4;92:18;103:1;
110:21;128:16;134:3;
149:6;152:14;153:6;154:3,
9,11,21;155:4;157:14,20;
159:18;164:8
depended (1)
148:21
depicted (1)
37:2
depicts (2)
35:11,13
deploy (1)
155:17
deployed (7)
12:1;98:5,7;119:17;
132:12;162:16;165:14
deployment (9)
7:1,12;60:2;97:5,7;
130:15;140:4;146:5;160:12
deployments (1)
132:12
deprived (3)
22:7;40:17;68:13
deputy (2)
23:8;107:16
derived (1)
37:16
describe (2)
9:18;37:9
described (8)
46:7;69:3;78:16;123:17;
148:7;155:4;161:16;166:11
describes (1)
28:19
describing (1)
78:11
description (2)
41:14;111:4
deserved (1)
40:18
design (1)
12:3
designed (2)
57:17;80:8
desire (1)
166:18
desired (2)
150:8;163:16
desires (1)
119:9
desktop (1)
73:13
desperately (1)
40:15
despite (2)
49:4;165:1
destroy (1)
39:4
detail (3)
5:12;28:19;136:19
detailed (6)
24:13;26:5;64:19;70:16;
95:16;123:2
detailing (1)
20:15
details (3)
131:1,3;156:2
detained (1)
10:1
Detainee (4)
59:12;60:9;69:18;129:2
detainees (2)
60:13;129:4
detainee's (1)
60:13
determination (1)
94:1
determine (3)
7:3,8;57:4
determined (5)
25:6;26:14;44:18;156:10;
166:17
develop (2)
30:12;156:6
developed (1)
142:5
devoted (3)
21:21;68:5;94:16
died (1)

9:5
different (16)
6:7,13;11:3;14:5;52:18;
57:21;86:2,3,3;89:10;
116:10;138:6;141:6;142:9;
146:4;154:4
difficult (2)
55:18;82:16
digital (1)
153:4
dikes (1)
166:12
diligence (1)
11:19
Diplomacy (12)
76:13,16;77:10;78:10;
82:5,6,9;86:13;95:12,13;
96:2;129:8
Diplomasy (2)
95:20;96:10
diplomatic (2)
79:6;80:10
diplomats (3)
131:6;149:9;158:5
direct (4)
9:8;53:21;54:7;146:3
directed (1)
159:14
direction (1)
6:8
directly (4)
87:10,12,20;102:21
directory (3)
110:11;112:13;118:13
discipline (1)
131:14
DISCLAIMER (1)
2:1
disclose (5)
136:2;146:19;161:11;
163:17,21
disclosed (12)
8:8;28:5;34:11;37:8;
117:6;139:11;144:6;
145:10,18;149:1;153:18;
160:15
disclosing (7)
17:19;20:13;109:3;139:1;
141:19;146:7,12
disclosure (9)
45:3;75:2;113:16;117:21;
138:14;139:16;146:1;
147:9;152:6
disclosures (4)
20:21;127:5;135:20;
161:10
discover (1)
137:9
discrediting (1)
133:21
discuss (3)
30:1;71:11;137:12
discussed (8)
37:19;43:17;59:16;66:8;
125:14;142:13;144:3;145:6
discussing (3)
34:12;126:19;150:21
discussions (1)
157:21
disk (13)
16:2,6;39:19;40:8;51:2,9,
12,15,20,21;81:12;86:9;
163:18
disks (1)
12:15
display (1)
35:11
displayed (2)
18:4;65:11
displays (1)
65:10
disposition (1)
60:13
dispute (3)
135:9,11;152:12
Disregarding (1)
38:1
disseminating (1)
81:20
distinction (1)
101:2
distinguished (1)
101:4
distraction (1)
133:12
distribution (1)
81:13
division (1)
155:17
divulging (1)
162:7
DOC (1)
32:9
doctoring (1)
38:11
document (46)
4:14;18:2;25:10;26:18;
27:2,13,14,14,19,19;28:6,6,
17;30:10,18;31:7,18;32:4,4,
7,8,9;33:11,13,14,15;34:15,
19;40:6;55:19;61:19,20;
65:16;74:8;96:7;126:21;
142:15,15,18;143:10,20,21;
144:9;147:12;151:19;
154:13
documents (72)
4:12;17:13;18:13;21:5;
22:10,11,14,16,18;23:1,10;
25:4,14;26:13;27:8;31:1;
35:16;39:19;45:20;48:14;
59:8,10;67:6;69:6;71:2,2,5,
8;72:9;73:14,16;74:5;
75:19;85:14;88:6;92:8;
96:5;104:1,9,14;105:8;
106:4,5,6,10,19;107:9,13,
18,20;108:4,5;114:10;
126:6;127:7,11,15;129:18;
130:15,16,16,17,17;136:2;
141:1;143:1;146:8,13,16;
163:17;165:13,17
DoD (6)
29:13,18;30:1,7;64:13;
160:17
Doe (4)
110:16,18,18,19
domain (1)
110:9
done (2)
105:6;117:20
dot (65)
13:15,15,16;14:9,10,11,
15;17:13;18:2;19:14,17;
32:7,11,19,19;40:5;43:10;
47:9;48:21,21;54:15,18;
64:6,13,16;65:1,10;72:14,
14,15;73:1,6,13,14;74:4,5,7,
9,11;76:2;85:15;89:10;
91:15,16;92:3,10,11,13,14;
93:12,13;104:12;108:19,21;
110:15,16,18,18,19;116:6;
143:17,18,18,18,19
double (1)
65:4
doubt (3)
136:1;139:4;166:8
doubted (1)
145:3
down (6)
19:11;49:21;50:2;88:7;
106:15;115:1
download (18)
10:7;50:21;62:7,8,20;
63:7,11,15;65:19;73:16;
84:2;87:21;103:21;105:7;
117:8;118:9,11;120:15
downloaded (16)
12:14;32:4;51:8;63:10;
73:11;83:15;85:7;104:4,9,
14,20;105:3;118:17;144:5;
145:9;162:17
downloading (7)
62:12;64:18;65:1;83:14;
87:8;102:11;116:1
downloads (1)
63:17
dozens (1)
121:7
draft (1)
2:12
draw-down (1)
132:9
drills (1)
155:15
drive (9)
38:17,18;43:15;50:17;
61:15;85:20;86:1;100:9;
141:7
Drum (3)
10:12;132:10;140:5
due (1)
2:17
duly (1)
79:15
dump (3)
55:5,8,12
during (16)
6:21;15:2,2;33:6;39:3;
72:19;97:4;105:10;125:6;
130:15;140:4;146:5;151:7;
154:7;160:12;165:13
DUST (1)
9:17
duty (5)
9:16;111:4;123:8;162:3,3

E

E4 (3)
69:13,14;122:1
earlier (9)
87:7;92:20;103:6;104:16,
21;105:21;106:12;143:14;
160:13
early (1)
82:1
earned (2)
69:14;122:1
earth (2)
131:11;149:7
easier (1)
47:16
easily (1)
146:2
easy (1)
47:17
edge (1)
149:21
edited (6)
34:21;41:19;43:10;44:2;
153:17;157:3
editing (5)
2:7,14;41:4;42:16;43:18
edition (1)
159:4
editor@wikileaksorg (1)
109:1
editorial (2)
30:3;143:5
edits (2)
41:11,13
effect (2)
94:2;105:21
effective (1)
50:6
effectively (2)
48:20;78:5
effectiveness (1)
113:1
effects (5)
105:20;138:13;149:4;
150:4;161:10
efficient (1)

87:3
efficiently (1)
30:12
effort (2)
43:12;166:19
efforts (2)
70:15;162:10
Ehresman (2)
96:17,20
either (3)
79:16;117:10;119:9
electronic (2)
119:21;120:12
elevate (1)
52:10
elevated (1)
99:7
elicited (1)
151:1
else (6)
5:5;19:20;67:4;97:18;
113:15;150:18
Elten (1)
3:8
e-mail (21)
41:8,10,12;43:18;80:16;
108:19,21;110:13;111:11,
21;114:8;117:2,11;118:8,
12;120:18;122:7;137:13;
143:11,17,18
e-mailing (1)
119:9
e-mails (13)
110:11;111:1;112:10;
115:8;116:1,5,14;117:4;
118:11;121:5,14;150:14;
165:3
embedded (1)
37:13
eminently (1)
130:10
emphasized (1)
123:3
employ (5)
6:16;9:19;10:15;146:18;
156:7
employed (1)
7:5
employees (1)
124:2
enable (1)
78:4
EnCase (2)
54:13;55:14
enclosures (2)
16:19;27:3
encoding (1)
90:19
encourage (1)
147:1
encouraging (1)
146:9
encrypted (3)
14:5;17:21;39:10
encrypting (1)
161:19
encryption (2)
46:7,8
end (9)
63:4;69:5;91:7;97:9;
114:17;123:11;143:15;
145:13;148:3
endeavor (1)
165:1
ended (3)
97:8,9;119:12
enemies (22)
5:13,13;8:5,19;9:6;18:16,
18;28:2;34:18;134:10,12,
17;136:19;139:19;154:4;
155:19;160:5;163:6;164:4;
165:16,19,19
enemiesal-Qaeda (1)
135:13
enemy (64)
4:21;5:9;6:4,4,6,10,14;
7:2,4,14,18;8:1;11:7;37:20;
75:8;130:3;131:2;134:1,7,
18;135:8,16,18;136:4,9;
137:9,16,17;139:5;140:3,
10,12,16;141:11,12,15;
142:1,4,10;146:15,20;
147:2,10;149:15;152:19;
154:16;155:8,9,12,16,21;
156:3,5;158:14,15,18;
159:20;160:1,4,8;162:6;
163:15;166:1;167:1
enemy's (4)
42:9;136:11;137:4;
158:11
energies (1)
113:18
engaged (2)
127:6;140:16
engagement (1)
37:10
engagements (1)
9:15
engineer (1)
54:2
engineering (2)
82:2;98:16
enough (5)
40:11;81:15;87:3,4;
144:14
ensure (2)
80:10;167:1
Ensuring (2)
79:19;137:21
entered (1)
121:11
entering (1)
121:8
entire (16)
40:12;45:4;50:8;62:7;
68:19;77:9;97:4;98:18;
111:10,18;130:21;131:8;
132:17;136:18;149:11;
165:1
entirely (1)
113:9
entirety (3)
37:6;65:15;82:3
entities (1)
150:8
entity (1)
110:9
entries (3)
111:10;121:20;122:5
entry (1)
121:17
enumerated (1)
33:14
environment (3)
157:18,18;158:1
equipment (1)
29:5
equipping (1)
52:17
equity (1)
72:9
erase (2)
16:6;47:5
erased (3)
17:7;20:11;39:3
erasure (1)
47:4
errors (2)
62:15;65:21
especially (4)
8:21;37:18;106:1;109:4
essential (1)
145:13
essentially (6)
4:9;14:13;33:4;39:10;
83:12;159:15
established (3)
121:2;136:9,12
establishing (1)
134:16
evaluation (2)
25:9;26:17
Eve (1)
33:11
even (21)
7:13;11:19;20:19;37:9;
42:12;44:8;45:2;55:11;
59:19;97:18;101:18;102:6;
107:4;118:11;120:17;
130:20;131:10;149:17;
152:7;158:2,6
event (5)
5:3;6:21;39:12;114:9;
156:21
events (8)
5:19;6:3;14:9,10,10;
128:10,14;157:16
everybody (2)
131:11;149:7
everyone (2)
19:20;112:20
evidence (35)
12:16,17;15:6;16:12;
17:7;18:3;37:13;39:4;40:4;
45:16;47:6;54:4;67:5,10,
11;76:8;91:10;100:7,10,14,
16;116:16,21;118:1;121:3;
129:16;130:2,11;134:11,14;
135:18;136:6;141:17;
150:21;166:4
evil (3)
135:17;152:3,8
exact (10)
32:3;52:2;55:15;85:20;
88:3;105:11;114:10;
130:21;146:19;156:8
exactly (3)
52:15;153:13,14
examiner (1)
114:13
example (3)
5:2,20;6:19
examples (1)
78:9
exceed (1)
122:8
exceeded (1)
25:17
exceeds (1)
24:2
Excel (6)
11:12;14:13;88:16,17;
89:5;91:16
excels (1)
157:19
except (1)
50:2
excerpt (2)
73:6;104:8
excerpts (1)
154:1
exchange (5)
110:4;114:6;117:3;
120:17,18
exclusive (9)
8:7;22:4,7;68:10,13,14;
94:20;95:3;124:16
excuse (13)
14:9;17:4;27:15;51:8,12;
55:7;107:11;108:9;115:16;
122:12;141:1;157:10,17
excuses (1)
36:18
EXE (4)
64:13,16,19;65:1
executable (7)
64:12,17;85:4,13;89:8;
99:17;100:15
executes (1)
155:18
executing (1)
16:5

executive (1)
67:11
exercised (1)
84:9
exfiltrate (5)
20:17;113:21;114:2,5;
115:6
exfiltrating (2)
116:1;161:4
exfiltration (1)
84:11
Exhibit (111)
4:14;13:3;15:14,17,18;
16:3,4,15,16,18,19;19:8,14;
23:18;27:11,20,21;29:12;
30:16;31:15,20;32:1,13,21;
40:5;41:7;43:3;45:7;46:17,
18;47:20;51:14,15,18;
53:16;54:7,12;55:20;62:9,
16,17,19;63:5,15,19;64:2;
65:7;66:18,20;67:8,10;
70:8;71:15;72:2,5,7,11,18,
20,21;73:10,18;74:8,13,18;
75:12,13,17;79:12;84:15,
19;85:7;86:5;87:13;89:21;
90:3,11;91:13,19;92:2,9,13;
95:7;96:13;104:7,11,17,19;
105:13;113:20;114:11,18;
115:2,13;122:18;123:14;
134:21;135:2;137:6;139:6,
8,13;141:4;142:15;145:7;
153:12,21;154:7,13,19;
155:3
Exhibits (8)
75:6;78:6,14;111:7,8,9,
13;116:13
exist (1)
89:13
existence (1)
146:21
expected (4)
31:16;75:3;131:17;135:6
experience (9)
10:11;18:8,11;30:21;
42:8;44:9;84:7;140:3;
162:20
experiences (1)
35:17
expert (3)
99:18;106:18;140:14
explained (13)
7:2;28:13,17;36:11;52:4,
12;63:11;65:6;75:7;104:16;
106:11;111:20;135:6
explaining (1)
18:6
explains (3)
31:18;153:13,21
explanation (1)
17:6
explicitly (2)
127:1;142:10
exploitation (3)
112:18,21;164:17
Explorer (1)
73:9
export (10)
11:4,5,8,9,11,15;82:20;
83:1;116:8;118:10
exported (1)
68:20
exporting (2)
11:1;59:17
exposed (3)
119:15,19;120:10
exposes (1)
35:14
exposure (3)
10:18;38:4,5
extensive (2)
10:11;140:3
extent (2)
61:2;78:12
external (2)
141:7;146:1
extract (9)
54:11,18;62:18;65:17;
109:9,11;114:15;115:6;
123:18
extracted (6)
21:6;65:8;67:14;94:3;
109:12;124:7
extracts (4)
89:10;98:19;111:14,20
extremely (1)
8:14
extremist (1)
143:14
eyes (1)
133:14

F

Facebook (1)
44:3
faces (1)
155:19
facilitate (2)
36:1;118:5
fact (13)
8:21;12:17;47:18;87:6;
134:21;135:3;139:10;
148:14;153:1,12,20;154:6;
163:4
facts (5)
47:6;127:21;134:16;
135:9;150:20
factual (1)
156:5
fail (1)
49:4
failed (1)
63:3
failure (1)
63:13
fallout (1)
76:7
famous (1)
20:5
far (5)
24:1;25:17;38:9;66:15;
130:20
Farah (7)
103:3,10,15,20;104:3,5;
108:4
Fast (3)
57:4;87:3;113:16
faster (2)
64:3;85:2
fear (3)
58:16;145:17;146:2
feat (1)
11:14
feature (1)
11:5
features (1)
53:2
February (13)
15:7,9;16:1;32:10;35:6;
39:17,18;60:5;81:18;82:1;
93:7;144:5;145:9
feed (1)
2:6
feet (1)
101:18
FEIN (32)
3:4;4:5,6;15:18;23:15;
24:18;27:7;33:3;42:5;43:6;
45:12,15;46:15;51:19;
58:20;59:6,7;61:9;62:5,17;
71:19;72:21;92:6;93:1,3;
108:15;114:21;125:2;
126:4,12;128:8;167:7
fell (1)
132:1
fellow (4)
81:10;113:10;162:6;
166:11
felt (2)
69:5;132:21
few (2)
33:4;111:8
field (3)
5:16;22:12;115:2
fight (3)
18:18;113:9;155:12
fighting (1)
163:21
figure (7)
7:6;57:7;58:12;85:1;
88:20;115:5,20
file (63)
14:6,9,15,16;17:21;19:14,
17;40:7,7;49:18,19,19,19;
50:1,1,16,16;51:5;53:20;
54:18,19,21;55:6,12,13;
56:3;57:14;58:5,7;64:19;
65:7,9;72:13,18;73:2,2,6,7,
17;74:4,8;85:4,13;86:1,4;
88:20;89:7,10;91:15,17;
92:10,14,14,14,20;93:4,12,
14;104:12;105:2;115:10,
10;116:6
files (34)
14:5,12;46:10;48:11;
50:1,3,12;52:5;64:13,16,17;
73:3,8;85:17,18;86:6;89:7;
92:10;93:13;99:17;100:6,8;
101:3,5,6;104:5,20;105:3;
109:13;116:10,12,14;117:1,
2
final (1)
124:20
finally (9)
19:11;20:5;44:1;49:20;
89:4;99:16;108:3;132:13;
137:21
financial (2)
116:18;150:7
find (6)
57:2,7,9,11;149:11;166:7
finding (1)
52:10
finish (2)
124:20;125:20
finished (1)
24:14
Finkel (1)
37:11
firewall (3)
90:2,5,12
First (36)
6:18;7:11;10:15,20;11:9,
16;20:8;33:7;38:14;42:20;
49:9;57:20;62:2;63:14;
64:7;73:11,12;88:11;91:20;
97:5,7,8;110:15;111:21;
114:16;125:14;126:18;
136:16;142:12,13;144:3;
145:6;148:3,7;152:21;
153:5
five (4)
20:19;101:18;143:20;
160:13
flag (4)
151:5,8,9,10
Florinda (1)
97:11
flow (1)
13:2
flying (1)
35:10
FOB (4)
10:12,17;45:18;101:11
focus (4)
9:16;77:2;81:5,7
focused (4)
133:8;137:17,21;166:6
focusing (1)
163:20
fog (2)
18:17;141:2

FOI (1)
149:5
FOIA (3)
39:13;44:11,14
folder (17)
13:15,20;14:2,4;52:3;
73:14,20;74:1,2,6;85:14;
92:4,7;103:15,20;104:3,5
followed (2)
33:15;117:6
followers (1)
159:14
following (3)
29:4;54:21;127:21
footage (3)
35:2,21;39:18
force (2)
29:10;142:18
forces (12)
7:2,14;9:9;10:3;29:17;
80:20;114:6;118:4;132:8;
156:4,13;157:1
foreign (47)
22:2;24:4,8;25:3,6,12,19;
26:1,12,15,20;29:14,15;
30:7;68:8;70:5,11,14;75:1,
5;76:10,18;78:1,5;79:5,6;
94:18;95:10,14;96:11;
119:19;122:13,20;123:4;
124:14;128:21;129:7;
131:8;139:14;143:1,7;
149:12;150:7;157:16,17,21;
160:17
forensic (4)
16:16;40:4;54:13;114:13
forensically (4)
15:12;16:7;118:2;165:4
forensics (1)
55:15
forever (1)
20:16
form (3)
43:13;90:20;141:15
formal (1)
103:12
format (5)
90:18;131:9;149:12,14;
158:19
formation (1)
133:3
formatted (1)
117:4
former (2)
106:17;107:1
forms (1)
111:15
Fort (3)
1:11,17;10:12
forth (5)
25:2;26:11;70:20;95:20;
123:11
Fortunately (1)
49:2
forward (1)
17:4
found (16)
7:7;13:17;15:1;25:5;
26:14;40:8;59:14;60:9;
89:10;113:14;114:13;
117:3,6;131:7;152:10;
154:12
foundation (2)
133:4,15
founded (1)
143:14
four (5)
7:3;13:12;65:19;103:18;
160:13
fourth (1)
127:13
fox (2)
81:5;136:18
FPT (1)
49:3
free (4)
17:9;42:1;50:21;139:19
friends (1)
15:8
front (1)
133:14
fruit (1)
20:17
fruition (1)
132:15
fruits (1)
132:14
frustrated (1)
132:2
Ft (2)
132:10;140:5
FTP (13)
48:7,8,20;53:4,9,12;54:2,
19,20;55:3;56:8;57:9;58:9
fuck (1)
164:13
fucked (1)
164:8
fuel (1)
90:21
full (2)
97:8;111:3
Fulton (4)
6:11,13;38:16;43:14
function (9)
11:12;82:21;87:8;89:1;
115:7;116:7;118:10,10;
159:15
functionality (2)
84:3;89:13
functions (1)
99:9
funding (2)
80:3,5
funeral-like (1)
132:1
Further (7)
22:14;31:18;98:15;107:1;
141:13;142:5;159:10
Furthermore (5)
8:18;21:16;60:21;67:21;
94:11
future (2)
94:3;140:12

G

Gadahn (8)
134:16;135:3;153:17,20;
154:5,21;155:5;157:7
gain (6)
42:11;49:3;52:14;58:3,5;
81:13
GAL (17)
110:6,13;112:17;113:3;
114:5,15;122:6,8,10,15,15;
123:5,8,11;124:7,9,13
games (8)
99:13;100:5,8,11,15,17,
19;101:7
GAP (7)
84:12;109:9,11;120:6,8;
161:17;163:19
gaps (1)
61:1
garner (2)
40:13;60:4
garnered (1)
144:10
Garrison (2)
1:9;136:8
gather (5)
8:10;130:3;135:14;147:2;
153:6
gathered (1)
5:10
gave (5)
6:18;99:21;102:16;152:9;
165:16
general (4)
135:17;148:3;152:3,8
generalities (1)
80:12
generally (3)
9:14;30:20;71:11
geographic (1)
95:16
gets (1)
47:1
Gharani (6)
39:4,8;40:15;103:8,10;
106:1
given (4)
8:21;30:21;110:9;150:15
giving (6)
130:20;134:1;135:15,16;
142:1;147:12
glad (1)
43:19
Global (24)
108:7;109:12,15,17;
110:4;111:19;114:1,4,16,
21;116:10;117:19;118:5,
12;119:11;120:16,19;121:1,
9,13,16,20;147:14,16
globe (1)
81:3
gmail (2)
116:18;119:10
goal (1)
84:16
goes (4)
27:14;29:21;76:14;121:9
good (5)
58:17;125:3;131:14;
140:8;143:14
Google (3)
85:4;114:13;115:3
Government (37)
2:3;3:3;20:18;23:19;
29:7;31:8;34:1;37:5;52:18;
75:16;80:11;96:16;98:13;
108:4;110:7;117:7,9;
118:17;119:8;120:9;
123:19;124:2,17;125:16,16;
126:2;129:6;146:10;148:9;
150:2;153:2;154:8;160:7;
163:7,10,11;165:17
governments (1)
139:14
government's (2)
36:14;125:20
grab (1)
88:6
grade (3)
69:13;70:2;121:21
granted (2)
118:7;125:15
graphical (2)
65:2;89:19
graphics (1)
108:1
grieved (1)
132:2
group (1)
149:5
groups (4)
29:15;96:3;137:8;143:2
GTMO (13)
59:8,9,13;60:9;61:10,15,
16;66:14;69:2,6;70:15;
84:7;129:2
guarded (1)
78:4
GUI (1)
65:3
guide (2)
56:12,13
guilty (1)
166:8
gullable (1)
166:13
Gwynn (2)

28:7;31:6

H

ha (1)
47:21
habit (1)
102:5
habitual (1)
142:6
hacker (2)
166:11,11
hackers (1)
139:15
hailed (1)
40:20
haired (1)
161:19
Hall (6)
1:10;5:15,17;106:17;
140:14;158:13
Hammer (4)
10:12,17;45:18;101:11
hand (4)
53:11;70:8;95:7;122:18
handed (1)
23:17
handle (2)
56:13;106:19
handling (1)
44:16
hands (7)
9:5,6;112:11;136:4;
139:5;154:4;167:1
handy (1)
165:3
happen (1)
157:9
happened (2)
5:6;6:21
hard (5)
50:17;85:20,21;141:7;
162:5
harder (1)
163:10
harm (9)
5:13;23:2,12;75:4,4;
79:14,14;107:14;166:18
harvest (6)
65:14;77:12;81:12;87:4;
90:14;93:18
harvested (6)
89:18;91:3,9,10,20;
165:12
harvesting (2)
66:4;90:9
Harward (1)
107:16
hash (16)
49:12,12,13;53:8,10,19;
55:6,11;56:1,3,12,13;57:2,
4,13;58:8
hashed (2)
55:1,1
hashing (1)
46:10
head (1)
61:14
Headquarters (3)
1:8,8;77:18
hear (1)
98:8
heard (25)
9:13;13:16;14:12;31:6;
35:8;45:10,15;48:7;52:8;
98:6;103:6;110:20;117:3;
123:21;129:16;130:1;
134:10;140:11;151:6,16;
155:10;156:12,19;157:15;
160:13
Hearing (2)
1:15;56:2
heart (5)
47:1;131:6;148:11,20;
149:10
heedless (1)
130:9
held (7)
7:10;22:17;36:18;48:17;
145:17;148:1;163:2
helicopter (5)
35:3,9,12;42:17,21
helicopters (1)
35:11
help (6)
6:5;7:8;8:4;65:7,9;88:20
helped (1)
6:16
helpful (5)
152:19;155:8,9;159:9;
160:5
helping (2)
77:11;103:7
herring (1)
36:20
hex (4)
54:15;55:5,8,12
hide (3)
58:15;102:6;123:18
hiding (1)
47:7
high (1)
132:6
highest (1)
156:10
highlight (3)
46:2;66:15;69:6
highlights (1)
20:21
Hillary (3)
131:5;149:8;158:4
himself (13)
4:16;8:21;9:1;20:16;
34:17;36:9;41:10;42:12;
52:17;113:19;154:16;
156:16;158:2
historic (1)
18:6
historical (3)
8:12;18:12;135:7
history (2)
47:11;73:2
hit (4)
5:3;132:19,19;133:20
hits (3)
96:4,4;143:14
holder (1)
72:9
holding (1)
19:15
Holifeld (2)
12:5;13:8
Honor (318)
4:6,9;5:5,12,14;7:18;
8:18;9:7,13;10:5;12:13;
13:3;14:18;15:6;16:8,15;
17:7;18:4,14;19:7,9;20:1,7,
19;21:2;22:9;23:13,15,21;
24:14,19;25:3,13,15;27:1,
10,13,15,16,18;28:1,18;
29:9,21;30:15,17;31:15;
32:1,12;33:3,7,12;34:7,9,
19;35:8;36:10,15;39:1,7;
40:3,10;41:3,7,9,16;42:5,
10,13,20;43:6;44:15;45:1,9,
13,15;46:16;47:12,20;
48:19;49:16;50:4;51:7,14;
52:1,8;53:15;54:3,6,7,10,
20;55:2,7,16,19,21;56:10,
15;58:17;59:7,9,11;60:11,
21;61:13;62:1,6,17,19;63:1,
19;64:10,16;65:6,18;66:7,
20;67:19,21;68:15;69:5,11,
17;70:4,6,10;71:1,7,19;
72:3;73:1;74:3,15;75:3;
76:12,19;78:6,14;79:18;
81:9;82:4;83:4;84:8,15;
85:6,12;86:5,8,12;87:1,13;
88:2;89:12,21;90:19;91:13,
18,21;92:1,6,13,17;93:1,3,
13,17;95:5,9;96:9,12,14;
97:7,9,21;98:2,4,8,20;
99:18;100:7;101:13;102:4,
9;103:2,6,18;104:7,11,16;
105:10,19;106:10,17;107:4,
19;108:3,7,9,10,15,16;
109:2,10,19;110:15;111:3,
8,13,17;112:2,5,11,17;
113:21;114:8,12,21;115:4,
14;116:12;117:14;118:14;
120:7,15;121:4;122:10,12,
16,20;123:13,16,21;124:19;
125:2;126:4,9,12;127:14;
128:8,15;129:1,16;130:19;
131:12;133:11,17,20;134:1,
2,9,20;135:4;136:16;137:1;
138:5;139:4,9,10,20;141:5;
142:5,12;144:2,14,21;
145:5,12,20;147:5,9,18;
148:15;149:8,16;150:1,5,9;
151:2,16;152:4,12,21;
153:1,12,15;154:3,11;
155:6,10;156:8,15,19;
157:11,18;158:10,20;
159:18;160:21;161:13;
162:1,9;163:8,13,20;164:7,
11,15;165:1,18;166:3,10,
14,16,19;167:3,6,7
Honorable (1)
1:17
hooked (1)
12:11
horrifying (2)
147:16,17
Hoskins (2)
22:21;107:11
host (1)
47:6
hostile (1)
158:1
hour (4)
70:3;122:2,4;130:17
hourly (1)
69:17
hours (16)
16:6,9;39:17;51:10;57:8;
65:19;69:10,16,20,20;70:2;
90:8;104:4;121:15;122:4;
161:1
house (8)
15:1;17:18;19:15;21:14,
15;67:19;94:9;124:13
housed (1)
61:11
http (1)
143:17
human (2)
79:1;166:5
humanist (2)
147:20;166:10
hundreds (1)
11:1
HUNTER (1)
3:7
HURLEY (7)
3:13;23:16;27:12;70:7;
71:4;72:1;95:6
hyper-masculine (1)
166:12
hypocrisy (1)
41:17

I

IA (1)
120:12
Iceland (3)
77:2;81:2,2
icon (1)
65:4
ID (3)
61:19,20;65:16

identification (1)
137:19
identified (2)
6:15;78:21
identifier (2)
65:17;77:20
identifiers (1)
88:12
identify (2)
18:11;28:15
identity (2)
53:5;137:7
ideology (1)
157:19
idiots (1)
166:13
IED (3)
5:3,7;156:4
IEDs (3)
10:19;155:20;156:7
IED's (1)
156:11
ignorant (2)
141:8;166:13
ignored (2)
18:7;154:16
ignoring (1)
33:13
image (2)
51:5,5
images (2)
37:7;45:5
immediate (1)
43:12
immediately (1)
162:15
impact (4)
38:12;41:20;42:16;43:20
impacted (1)
133:3
impetus (1)
118:2
imply (1)
12:13
importance (3)
21:5;44:6;79:20
important (5)
4:17;55:9;63:1;92:19;
156:21
importantly (1)
46:16
impossible (1)
82:16
inaccessible (1)
12:3
inaudible (35)
2:17;8:11;9:11,16;10:3;
20:1;23:8;27:16;31:8,12;
33:16;35:11;40:3;42:19;
44:20,21;54:10;59:13;
63:20;64:11;67:15;100:5;
103:15;112:10;114:3;
118:11;120:21;130:8;
133:18,20,21;134:16;
147:13;157:14;161:7
incarceration (1)
79:2
incident (7)
36:16;37:2;39:13;103:14;
151:14,21;152:1
include (4)
10:1;93:8;100:8;139:16
included (9)
4:14;21:1;60:13;111:5;
126:21;144:15;149:15;
163:5;164:3
includes (6)
52:10;64:13;85:19;110:3;
137:19;145:18
including (11)
34:17;76:18;98:6;106:9;
111:4;119:17;137:8;
139:13;141:9,13;165:20
inclusion (1)
41:11
increase (4)
63:20;94:2;123:6;156:15
increased (2)
30:11;79:20
incredible (1)
150:17
increments (2)
11:6,10
independent (1)
121:2
in-depth (1)
155:4
index (4)
72:14;73:1,6;104:12
indicated (1)
67:6
indicators (1)
154:17
indiscriminately (1)
165:12
individual (6)
84:4;102:8,11;131:3;
146:3;155:16
individuals (6)
19:4;38:19;112:8;119:2;
123:1;145:15
individuals' (1)
111:3
individual's (1)
112:1
inevitably (1)
147:10
inference (1)
141:19
inflict (1)
155:12
information (248)
8:7,8,19;9:1,4,7;12:9;
18:9,15,21;19:18;20:5,8,11;
21:17;22:1,3,8,12;23:1,4,6,
17;24:5,9;25:4,20;26:2,13;
28:3;29:7,14,16,19;30:1,3,
8,12,19;31:1,2,13,19;34:4,
6;35:21;36:4,8,11;37:8,21;
41:17;42:1;44:6;47:4;
48:17;50:9;53:6,14;55:6;
56:9;57:10,18;58:1;59:14,
21;60:4,8,16,19;64:3;66:6,
9,16;67:3,13;68:1,6,9,14;
70:12,15;71:13,21;74:17,
21;75:7,9,21;76:1,6,9;78:3,
3,19;79:5,13,19;80:4,6,11;
81:2,20;82:15;83:2,7;
84:13;90:17,20;91:4;94:12,
17,19;95:4,11,15;107:3,13;
109:4,16,21;110:2,3,7,12;
111:5,18;112:8,19;113:13;
114:4,15;115:6;117:8,12,
13,14,20;118:15,18,18;
119:2,6,8,11,16,19;120:21;
121:2,9,12;122:7,15,21;
123:1,4,19,20;124:5,16;
129:11,19;133:4;134:4,8;
136:5,14,21;137:3,4,18,20;
138:1,14;139:2,4,11,17;
140:19;141:9,10,14,17,20,
21;142:1,7;143:2,4,8;
144:15;145:1,15,18,19;
146:2,10,11,19;147:2,13,
14;149:18,20;150:2,7,8,16;
152:5,6,7,13,19;154:4,9;
155:1,5,7,11,15;156:6,17;
158:12,18;159:9,16,19,20;
160:2,3,3,7,18;161:4;162:4,
5,18,21;163:7,10,12,13,18;
164:2,9;165:10,20;166:21
informations (1)
146:21
informed (2)
147:8;149:3
informing (1)
36:13
informs (1)
101:14
INFOSEC (3)
29:11;137:5;142:19
info-wise (1)
164:13
inherent (1)
21:4
inhibit (1)
82:15
injure (1)
76:10
inquires (1)
56:1
inscom (1)
143:18
insider (3)
131:18;146:1,1
insight (1)
8:1
insights (1)
5:19
Inspire (3)
158:20;159:1,3
install (3)
15:14;51:8;102:17
installation (1)
51:3
installed (5)
51:2;52:13;65:4;99:10;
102:14
Instead (9)
8:13;41:21;42:7;49:9;
77:11;81:9;120:7;130:21;
145:2
instructing (2)
41:11,15
instruction (1)
136:19
integral (1)
129:6
Intel (6)
32:5;43:2;48:4;53:14;
112:14;128:1
Intelink (13)
32:2;43:6;59:14;62:6,18;
63:3;72:8;105:13,15;144:4;
145:8;160:12;161:9
intellectual (1)
142:9
intelligence (94)
5:10,17;6:1;7:20;8:10;
11:5;19:4;22:3;24:4,8;25:3,
6,12,19;26:1,12,15,20;28:9;
29:15;30:13;34:11;44:21;
60:7,14,17,20;61:1;67:12;
68:9;69:10;70:5,11,14;
71:9;74:21;76:19;79:5,19;
80:2;81:11;94:19;95:10,14;
96:11;106:17,18;112:12;
119:20;122:13,20;123:4,6,
10;124:15;126:18;129:4,12,
12,13;130:4,7;134:2;
135:14,15,16;136:7,8,10,
17;138:20;141:14;143:1,
10;144:12;146:17;147:3;
148:3,7,9,13,16;149:16;
152:10,15,15,18;154:15;
155:6;159:21;161:6;163:3;
165:8,9
Intellipedia (2)
61:17,21
intend (1)
71:20
intended (5)
21:19;68:3;94:14;110:1;
118:16
intent (5)
20:15;134:5;135:17;
152:3,8
interest (3)
47:7;77:1;148:20
interested (1)
148:12
Interesting (3)

74:1,2;144:14
interests (1)
148:11
interface (5)
65:3;82:7;89:20;102:12;110:10
interfered (2)
68:17;95:2
internal (1)
131:17
internet (40)
30:19;31:10;46:3;47:9,10;51:1;73:2,8;90:21;116:20;119:13,14;120:10;126:9,17;127:17,19;129:14;130:3,8;137:4,5,13,15,16,18;138:1,4;139:16,17;141:13;142:5;145:12,14;147:1;149:1;158:21;159:5;160:4,16
interrupting (1)
42:4
in-theater (1)
147:7
intimately (1)
161:14
into (11)
5:19;18:3;39:21;49:17;84:4;88:16,19;89:6;90:17;91:11;103:12
introduce (3)
96:15,18;98:12
introduced (4)
64:8;85:11;97:15;100:12
introducing (3)
89:17;99:1,6
introduction (4)
100:18,18,19;101:2
intrusion (1)
120:12
invaluable (1)
7:17
invasion (1)
119:21
inventory (1)
4:10
investigation (6)
44:13;103:3,12,14;104:1;108:5
investigative (1)
104:5
involved (3)
5:7;24:12;26:4
involvement (1)
38:8
IP (2)
32:14,18
Iraq (28)
9:12;10:7,16;11:21;12:1,7;13:9;14:9;25:16;26:5;29:5;39:2;98:5;101:11;110:10,16;114:6;118:4,11;119:17;124:2;128:14;140:7,20;155:17,20;162:16;165:14
Iraqi (3)
19:19;80:19;132:8
IRQ (2)
14:10,15
IRR (3)
126:21;144:7,14
ISO (7)
51:3,3,4,9,12,21;52:2
isolated (2)
158:9;165:21
issue (3)
121:4;159:4,5
items (3)
18:6;43:1;153:4

J

JA (1)
54:8
January (24)
11:17;13:1,6,10,10,13,13,21;14:16,17;15:13;16:1,8;17:4,5,9,15;18:15;39:1,2,7;47:4;145:9;159:3
JDIMS-I (1)
61:15
Jihad (1)
159:7
Jihadist (1)
159:6
Jihadists (1)
157:7
job (2)
133:6,15
John (4)
35:9;90:15;110:15,18
Johnson (6)
16:10;66:3;74:7,11;116:21;117:3
join (2)
47:6;77:1
Joint (1)
1:10
JOSEPH (1)
3:5
JOSHUA (1)
3:12
journalist (1)
37:14
JRTC (1)
147:7
JTF (3)
61:10,16;66:13
Judge (14)
1:18;4:2;15:16;23:14;24:17;27:5;33:2;43:5;45:11,14;46:14;51:18;58:19,21
judgments (1)
29:8
judicial (4)
127:20;128:17;134:15,15
Julian (23)
33:21;47:19;49:5;53:19,21;54:17;55:11;56:7,11;57:9;58:11;59:17;66:5,7;69:2;116:19;127:4,6,13;145:1;148:5;162:2;163:2
Juliet (2)
16:15,16
July (3)
1:16;128:5,8
jumped (3)
109:3;138:8;157:12
junior (1)
158:13
justifications (1)
150:19

K

keep (4)
58:18;113:12;125:2;136:21
keeping (1)
165:3
kept (4)
20:11;141:6,9;145:1
key (7)
9:14;29:8;35:15;54:3;82:19;96:3,8
keyboard (3)
48:12,16,18
keys (1)
48:21
Kits (2)
97:13;99:18
KN (1)
56:1
knew (52)
14:18;19:3,3;22:9;23:6;30:6;31:3;37:20;42:17;44:5,10;57:15;84:1,6;87:1,2;96:15;97:19;101:14;106:3;120:12;126:7,15;127:16;129:17,21;130:2,20;136:4,13,13;138:5;139:3;141:19,20;146:8,13,19,21;147:13;148:1;149:6,15;150:3;157:9;158:17;160:1,4,6,15,16;164:3
knowing (8)
8:9;19:10;28:5;50:11;112:7;134:7;163:5;164:1
knowingly (4)
71:7;152:8;161:6;165:16
knowledge (19)
28:2;44:9;100:6;101:14;134:5;135:11,12;136:9;138:13,19;139:21;141:18;142:4;147:9,12;149:3;163:9;166:5,17
knowledgeable (1)
50:20
known (4)
9:17;57:2,3,4
knows (1)
155:16

L

labor (1)
20:17
labors (1)
132:14
Laden (10)
9:1;135:1;137:8;139:11;153:2,13;154:5,7;158:6;165:20
Lama (1)
81:14
Lamo (22)
14:3;20:20;21:2;59:20;66:13;84:14,16;116:18;120:1;131:5;147:18;149:3;151:1,3;158:3;160:21;161:13;162:8,13;164:11,15;166:14
laptop (3)
21:14;67:20;124:13
large (4)
20:8;130:21;145:21;159:9
largely (1)
144:13
LaRue (3)
35:9,20;36:11
laser (1)
35:14
last (9)
4:4;13:9;14:15;49:20;59:5;122:16;125:10;131:17;157:11
Lastly (1)
131:12
late (4)
10:21;18:15;82:1;103:7
later (13)
13:13,17;14:17;20:15,19;39:17;41:5;43:16;44:18;63:9;74:4;76:6;126:20
laughing (1)
34:3
Lauren (1)
162:2
layer (2)
49:20;90:19
lead (1)
156:14
leader (1)
9:14
leaders (4)
157:17,17,21;165:10
leading (3)
41:21;141:18;144:9
leak (2)
39:9;146:2

leaked (1)
145:15
leaks (4)
139:16,16;146:9;161:6
learn (5)
40:3;137:1;142:17;144:7;
145:11
learned (4)
36:1;130:21;137:5;
138:10
least (12)
24:20;25:7;26:8,15;
52:15;75:10;121:13;
130:12;152:20;164:14;
165:19,19
leave (3)
15:21;39:3;81:17
left (14)
15:21;17:17;33:6;39:2;
55:3,7,7,16;56:6;87:17;
91:15;92:20;113:6;133:13
legally (1)
145:17
legend (1)
71:16
legitimate (1)
119:4
less (6)
39:17;45:17;65:19;
105:20;138:8;148:8
lesson (1)
137:5
lessons (7)
36:1;137:7,8,12,16,17,21
letter (2)
153:5,8
letters (1)
49:11
level (7)
23:11;31:20;60:14;61:7;
107:18;110:8;136:19
levels (1)
80:11
Lewis (25)
22:2;23:21;24:3,19;25:1,
5,15,18;26:7,10,14;68:8;
70:10,17,19;94:18;95:9,18;
96:1,6,10;122:13;123:3,9;
124:14
Lewis' (2)
25:9;26:17
liable (1)
145:17
Lieutenant (5)
22:20,21;34:1;107:11,12
light (5)
125:19;132:17;147:6;
157:1,2
likely (5)
17:12;29:18;72:15;112:9;
120:10
Lim (7)
9:21;80:15,18,21;82:17;
83:17;143:12
limit (1)
121:5
limitation (4)
12:4;83:20;91:3;115:21
limitations (1)
36:14
limited (3)
78:12;82:9;145:19
Lind (1)
1:18
line (13)
40:6,6;46:17,17;62:19;
65:11;72:7,10;88:19;91:21;
93:16;110:15;158:3
lines (6)
16:4;43:3;51:16,19;89:5;
105:14
link (6)
43:2,14;48:4;53:14;
61:20;88:18
links (1)
80:14
Linux (10)
50:19,21;51:8,11,12,21;
52:2,6,17;57:19
list (28)
88:11;108:7,20;109:13,
16,17;110:5;111:19;112:9,
12,18,20;114:1,5,17,21;
116:11;117:20;118:5,13;
119:11;120:16,20;121:1,10,
14,17,20
listed (2)
112:7;118:12
listening (1)
2:6
listing (2)
110:8;111:10
lists (2)
159:6,10
Little (2)
55:18;67:12
live (2)
2:6;42:10
lives (1)
8:17
LM (6)
49:12,13;53:8,10;56:12,
13
load (1)
86:19
loaded (2)
39:21;86:20
local (4)
10:1;12:14;48:6;58:13
locally (1)
61:14
locate (1)
9:19
located (10)
7:4;12:11;17:21;22:14;
38:17;93:13;103:16,20;
106:10;153:3
location (4)
85:20;86:3;112:4;137:20
locations (2)
61:11;86:7
locking (1)
102:5
locks (2)
49:21;50:2
log (8)
16:2,11;51:15,20;62:18;
63:3;110:19;114:9
logging (1)
48:1
log-in (1)
53:5
logs (17)
9:15;13:1,4,7;15:14;32:2,
21;43:7;48:1,3;62:6;72:8;
75:18;90:2;104:8,19;
105:14
long (1)
161:21
longer (1)
148:19
longstanding (1)
112:9
look (5)
23:17;54:10;55:9;125:13;
133:13
looked (1)
75:19
looking (8)
24:14;57:11;59:21;60:3;
73:6;111:16;115:3;133:14
lost (1)
113:11
low (1)
123:11
lowest (2)
69:11;70:2
loyalty (2)
148:19;165:15
luckily (1)
57:10

M

ma'am (5)
15:18;24:18;27:7;46:15;
58:20
Mac (6)
47:4;51:16,20;56:17;
92:16;163:19
machine (6)
16:7;47:17;73:5;74:12;
110:9;165:4
Macintosh (3)
16:17;74:10;76:3
Macro (2)
114:17;115:1
macros (2)
109:9;116:3
Madaras (1)
81:4
magazine (6)
158:20,20;159:1,3,6,8
main (4)
5:20;12:2;29:9;98:21
maintain (1)
113:15
maintained (1)
12:6
MAJOR (12)
3:4,13;4:5;23:16;27:12;
59:6;70:7;71:4;72:1;95:6;
144:11;152:1
makes (4)
33:18;71:9;112:7;154:14
making (1)
165:2
manage (1)
82:16
manager (1)
9:10
managing (1)
162:11
Mander (1)
14:21
manifested (1)
152:4
manipulate (1)
117:8
manner (5)
35:19;109:21;118:1,16;
164:20
MANNING (332)
1:6;4:16;6:15;7:12;8:8;
9:3;10:6,11,13,17,18,20;
11:9,21;12:14;13:8,11,14;
14:3,18;15:3,8,10,11,21;
16:5,11;17:7,16;18:1,5,14;
19:9;20:8,9,16,20;21:6,13,
16,19;22:9;23:6,15;27:6,11;
28:2,5;30:6,18;31:13;32:3,
6,14;33:5,8,10,12,18,21;
34:16,21;35:1;37:19;38:2,
10,14,20;39:2,8,12,16;
40:12,14,17,21;41:3,8,9,18;
42:20;43:8,13,17;44:2,5,18;
45:16;46:2,6,7,12,20;47:2,
13,21;48:6,21;50:5;51:8,21;
52:3,15,19;53:1,8,11,18;
54:1,14;55:10;56:1,7,16,20;
57:6,11,15;58:9,12;59:13,
19;60:7;62:1,12;63:2,9,18,
20;64:2,6,7;65:1,13,15,18;
66:4,7,13,14;67:14,19,21;
68:3,16,20;69:5,18;71:4,7;
72:1;73:11,14;75:19;76:1,6,
20;77:3,3,4,7,8,11;81:11,14,
21;82:2;83:15,20;84:1,9,11,
18,19;85:4,7;86:9,9;87:1,9,
15,17;88:2,9,17;89:1,4,12,
16;90:8,13;91:3,8,19;92:20;
93:10,17,17;94:4,9,11,14;

95:2;96:15;97:8,15;99:4;
101:12,13;102:5,10,13;
103:7,19;104:3,4,9,14,19;
105:1,15,19;106:3;107:2;
109:2,9,12,20;111:19;
113:6,8,14,17,21;114:3;
115:20;116:17;117:1,6,16;
118:17,21;119:6,15;120:1,
4,7;121:17;122:8,11;
123:16;124:1,7,12;126:5,
14;127:1,5,15,18;129:13,
13,17,20;130:2,6,14;131:3;
134:2;135:12,17;136:4,6;
137:1;138:5,18;139:2,12;
140:1,15,18;141:6,18;
142:13,17;143:9,11,20;
144:3,17;146:4,13,18,21;
147:13;148:1,6,21;150:6,
10,11,15;151:4,9;152:3,8;
153:18;154:10,16;155:1,21;
156:9;157:9,14;158:2,11,
17;159:13,15;160:1,10,20;
161:3,12;162:7,14;163:9,
16;164:21;165:7,16;166:10
Manning's (54)
4:10;12:20;13:5;15:1,15,
20;16:2,16;38:8;44:1,4,15;
47:7;49:3;51:16;54:17;
62:9,20;65:8;66:1;72:14;
74:5;81:7;85:10,15,16;
86:7;90:4,15;92:8,16;
104:13,17;107:4;108:11;
118:14;120:10;131:13,21;
132:5,16,20;133:2,19;
135:11;136:1,16;142:4;
143:19;145:6;147:6;
148:15;149:2;166:7
manual (2)
62:9;65:20
manually (1)
84:2
many (11)
33:2;65:11;69:7;104:13;
107:1;108:19,20;112:6;
138:9;139:19;157:12
map (4)
6:3;17:2;51:13;112:15
March (45)
17:1;28:18;32:10,16,17;
43:1;45:19;46:5,11,15;48:3,
5;51:10;53:17,18;56:10;
62:3,6,13,19;64:4,7;65:21;
66:1;72:10,16;73:12,15,21;
74:10,13;82:1;85:1,3,3,10;
90:6,6,14;91:8;93:9,10;
97:10;127:21;143:11
marine (1)
8:10
marked (7)
22:11;31:11;66:21;74:16;
106:5,7;114:18
markings (4)
31:3;106:8,9,20
martial (2)
97:20;165:19
Martin (1)
143:12
Maryland (4)
1:17;15:2,21;17:18
mass (5)
87:8,21;116:7;118:8;
144:9
massive (1)
162:8
Master (2)
151:14,17
match (1)
43:15
material (13)
37:1,5;38:2,13;39:20;
44:5;117:7;137:15;138:4;
155:8;156:17;158:7,8
materials (1)
147:11
mathematical (1)
49:13
matter (2)
1:15;77:2
maximize (1)
41:19
maximum (3)
38:4,5,12
may (20)
2:13;20:20;23:13;43:17;
71:3;85:11;90:13;92:3,6,10,
15;93:9,11;108:20;109:8,
12;113:6,7;153:2;156:14
McNamara (4)
39:21;46:8;151:1;162:2
MD5 (1)
46:9
Meade (1)
1:17
mean (2)
56:5;109:10
meaning (1)
120:8
means (3)
52:13;146:17;152:18
meant (3)
40:17;151:9,10
measuring (3)
13:1;45:3;128:1
mechanism (3)
58:2,10;88:3
mechanisms (1)
99:8
media (7)
2:5;42:4;144:11;153:4,5,
16;156:20
meet (1)
129:20
meetings (1)
78:21
member (3)
153:5,6,8
members (7)
9:19,20;10:17;35:17;
120:11;121:8;134:17
memoranda (11)
72:3,15;73:5;74:15,16;
75:3,8,9,11,15;76:4
memorandum (6)
73:11,12,13,17,20,21
memorialize (1)
20:16
memory (2)
85:19;151:17
mentioned (5)
73:7;87:7;112:1;114:1;
150:12
mentions (1)
37:14
mentor (1)
80:19
mess (1)
162:8
message (3)
77:16,20;91:1
messages (1)
114:9
met (1)
125:12
method (6)
50:6;62:13,15;82:2;
84:10;114:9
methodically (1)
141:9
methodology (1)
141:12
methods (5)
37:15;45:6;75:1;79:6;
146:17
meticulous (1)
28:11
metrics (1)
35:15
Microsoft (16)
32:8;49:7,16;50:8,12;
53:2;73:8;85:17;88:17;
91:16;110:4;114:6;115:16,
17,18;118:9
might (1)
47:13
migration (1)
72:18
mil (4)
108:19,21;110:16;143:18
military (16)
5:2;8:15;24:9,12;26:2,5;
103:9,11;105:8;106:1;
128:4;133:5,15;136:16;
137:10;141:6
Miller (13)
6:14,16;100:2,4;131:16,
16,20;132:4,18,18;133:3,
10,17
Milliman (4)
96:21;97:2,3;98:7
million (5)
25:11;26:19;84:2;89:16;
96:11
mine (3)
147:2;158:12;159:16
minimum (3)
70:1;146:8,13
minimums (2)
24:2;25:17
mining (6)
72:14;140:9,10;141:14;
158:16;161:15
minute (2)
63:9;130:18
minutes (8)
16:6;35:2;56:19;58:19;
59:1;63:18;121:13,15
mIRC (4)
99:19;100:3;101:8;102:1
misconduct (3)
131:13;132:5,17
missing (3)
2:16;9:18,19
mission (16)
9:15;28:13;35:18;80:17,
18;81:1,10;83:3;91:8;
100:3;102:17;126:19;
132:7;133:8;155:18;163:21
missions (2)
19:21;113:1
misspelled (1)
2:15
misuse (1)
109:15
Mitchell (1)
151:14
Moats (5)
61:13,18;69:8,11,19
mock (1)
20:14
modified (1)
52:13
moment (4)
23:13;43:19;92:2;112:1
money (2)
24:6;150:17
monitor (1)
33:19
monitoring (1)
105:17
month (6)
69:15;97:5,7,8;122:2;
130:16
monthly (1)
11:10
months (8)
11:3;20:19;66:12;103:18;
161:2,3,5,8
morale (5)
100:5;132:6,19;133:19;
156:14
more (32)
4:11;8:2;10:8,10;11:19;

14:19;18:12;30:12,20; 35:10;37:18;46:16;77:7; 81:21;90:5;91:9;94:2; 104:4;112:8;121:5;123:4; 126:5;128:5,11;129:2; 130:14,17;141:1;148:10; 160:11;163:10,11
Moreover (2)
37:11;112:11
morning (3)
131:7;143:15;149:11
MORROW (1)
3:5
MOS (1)
136:18
most (9)
29:18;41:2;50:6;73:19; 113:8;132:12;140:21; 158:9;165:21
mostly (1)
27:16
motivated (1)
42:15
motivation (1)
150:13
Mountain (5)
6:12;7:21;98:5;139:21; 147:7
Mountain's (1)
100:3
mounting (1)
92:11
mouse (1)
42:14
move (2)
27:1;113:8
moved (5)
73:20,21;76:3;92:16; 117:1
movements (4)
9:16;107:21;108:1; 140:17
movie (1)
100:7
movies (8)
100:4,8,11,15,17,19; 101:7,7
moving (5)
73:3;101:4,6;113:16; 163:17
MRNs (3)
88:12,15,18
much (4)
42:1;60:4;66:1;91:3
multiple (14)
24:4;25:19;49:7;51:9; 70:11;95:10;106:14; 107:19;122:14;134:11,11; 146:5;165:2,9
Murder (2)
41:6;43:10
Murder' (1)
105:16
Murphy (1)
79:11
music (7)
99:13;100:4,8,11,15,17, 19
must (7)
30:6;78:4;139:17,18; 143:6,6;155:7
Myer (1)
1:11
Myer-Henderson (1)
1:10
myth (1)
36:19

N

naive (5)
42:6;141:8;162:16;164:5, 18
naivety (1)
164:21
name (12)
14:15;40:7,7;41:5;48:8; 58:2;74:1,2,5;112:1,3; 114:19
named (10)
13:15;19:4;48:7;72:13; 73:20;74:1,9;91:14;92:14; 103:15
names (20)
2:15;9:18;10:1;14:9; 72:18;73:17,17;78:18,21; 110:17,19;111:1,3,11; 112:6,7;116:13;117:1,4; 119:18
nation (4)
76:11;162:19;163:7; 165:15
national (16)
22:20;23:2,12;31:5,19; 34:12;61:6;74:17;75:4; 79:15;107:10,14;144:18; 148:11,17,20
nationals (1)
10:2
nation's (3)
138:16;147:1,10
nature (6)
4:13;28:20;38:13;130:9; 141:3;166:5
navigate (2)
50:16;86:17
navigating (1)
58:7
NC (1)
13:16
NCD (34)
77:9;78:11;79:19;80:5,7, 13,16,21;81:5,9;82:3,9,13, 17,18,19;83:5,13,14,18; 87:2,7,10;89:19;90:14; 91:20;94:4,6,12,17;102:11, 12,21;129:10
NCD's (1)
84:3
NCIRR (1)
144:2
NCIS (1)
144:15
nearly (1)
91:7
necessarily (3)
6:20;27:2;67:9
necessary (3)
8:5;80:4;135:18
need (7)
10:14;21:11;33:19;37:21; 80:2;137:2;167:5
needed (3)
41:17;67:9;113:12
need-to-know (2)
67:18;94:8
negative (1)
157:2
negatively (1)
133:2
Nehring (1)
22:21
neighboring (1)
10:3
neither (1)
34:5
Neri (2)
107:11,12
net (3)
13:1;95:13;108:18
Net-Centric (12)
76:13,16;77:9;78:10; 82:5,6,9;86:13;95:11,19; 96:2,10
Network (6)
9:8;52:20;59:15;101:5; 119:8;161:18
networks (10)
11:20;98:2,10,11;161:1, 15,17;162:11,12;163:1
New (3)
34:3;121:11,13
newest (1)
88:14
news (1)
144:11
next (11)
4:6;27:13;34:19;39:15; 45:9;59:7,9;63:12;76:12; 93:15;103:2
NIPRNET (8)
84:20;85:8;109:15; 110:18,19;113:18;118:9; 124:3
Nixon (5)
110:6;118:3,7;120:14; 121:7
non-disclosure (4)
107:5;138:10,12,18
None (1)
135:9
nor (1)
119:1
normal (2)
58:4;83:14
normally (1)
58:14
north (2)
143:17;144:13
notable (1)
60:3
note (7)
18:5,5;41:9,16;51:14; 56:15;82:4
noted (3)
104:21;120:4;149:8
notes (1)
2:14
notice (4)
127:20;128:17;134:15,15
notified (1)
151:14
noting (1)
43:15
notoriety (7)
19:12;38:6;40:18;42:16; 43:12;77:7;81:13
notwithstanding (1)
38:12
November (7)
32:20;33:4,10;97:9; 128:15;142:14;145:2
number (25)
24:13;26:6;55:17;56:6; 61:19,20;65:16;70:16,20; 77:20;90:1;91:1;92:1,19, 21;93:4,11,15,16;95:17,21; 123:2,12;138:7;157:11
numbers (1)
49:11
numerous (1)
132:11

O

obfuscate (1)
47:16
obfuscating (1)
46:3
objective (1)
28:17
OBL (2)
8:21;9:5
obliged (3)
21:20;68:4;94:15
observed (1)
81:19
obsessed (1)
47:2
obsessively (1)
33:15
obtain (5)

35:15;43:12;52:5,21;
86:10
obtained (4)
28:4;53:8,20;57:13
obtaining (3)
19:11;49:15;58:8
obvious (3)
46:21;105:5;158:6
obviously (1)
157:4
OCA (5)
23:9;61:5;79:15;106:20;
107:17
occasionally (1)
143:13
occasions (2)
143:21;146:5
occur (2)
89:2;136:5
occurred (9)
12:17;15:7,9;16:13;
17:14;47:13;56:16,18;
151:20
occurring (2)
128:10,14
October (1)
128:11
off (9)
6:15;10:14;16:10;56:16;
70:2;113:17;117:17;
133:14;134:17
offense (2)
27:16;121:6
Office (6)
32:8;111:4;112:3;115:17,
18;144:16
Officer (2)
35:9;121:19
official (8)
2:3;34:1;72:4;75:16;
77:16;118:5;120:17;160:7
officially (1)
37:6
officials (3)
78:16;153:3;154:8
often (2)
5:18;78:2
OJ (2)
71:2,13
older (1)
7:13
Once (8)
17:16;19:5;30:20;65:19;
83:9;86:20;150:11;164:1
one (46)
4:11;16:8,21;40:20;
41:12;43:10;46:1;47:6;
48:13,16;49:18,18;50:19;
52:4,9;58:13;62:20;83:18;
84:4;97:18;98:4,21;99:19;
102:2,19,20;111:10,11;
113:4;121:16;124:20;
131:7,18;134:14;139:18;
140:8,21;141:1,8;149:10;
151:12;161:20;162:9,9;
163:18;164:19
ones (3)
111:16;127:8;161:15
online (2)
69:4;127:6
only (35)
7:16,18;12:10;13:4;17:6;
21:10;31:7;42:2;44:6;52:4;
58:5;67:17;80:14;82:5;
83:2,5,6,18;86:13;94:7;
98:11;99:9;102:13,20;
103:15;106:20;112:2;
116:5;124:10,10;141:18;
145:21;148:11;164:13,21
on-the-job (1)
37:19
onto (17)
15:5;39:19;42:6;64:8;
74:12;85:7;87:20;91:5;
100:20;102:18,19;104:5;
110:19;119:10;121:9;
161:17;163:14
onward (1)
90:14
ooze (1)
163:14
op (2)
98:9;113:4
open (7)
37:1;42:18;43:8;71:11;
75:18,20;139:19
opening (1)
86:14
openly (1)
97:18
operate (3)
58:15;65:2;135:8
operated (2)
153:17;160:11
operating (10)
50:8,15,19;51:1,11,12;
52:6,18;53:3;58:1
operation (8)
12:7;24:11;81:8;103:9,
11;105:8;106:1;128:4
operational (4)
26:3;108:1;137:12;
162:12
operations (6)
9:11;24:12;26:5;28:20;
126:20;137:10
operator (1)
15:13
opportunity (4)
39:14;77:7,12;109:3
OPSEC (4)
29:11;139:7,15;142:19
option (1)
87:4
options (1)
65:11
order (36)
2:9;4:2;7:6;11:8;20:14;
23:16;39:4;52:13,21;57:2,6,
9,15;59:3;63:17,19;64:9;
65:14;84:9,12,13;88:5,6,8;
89:2;109:11;111:1;113:12;
115:5,18,20;125:8;131:14;
132:9;133:7;155:6
ordinary (1)
62:13
organic (2)
84:3;89:1
organization (5)
35:5;112:12;123:1;
141:20;153:16
organizational (1)
110:8
organizations (9)
5:9;8:9;34:14;60:18,20;
61:2;138:7,19;157:6
organized (1)
114:3
origin (1)
79:3
original (3)
27:20;31:17;125:17
originator (1)
78:19
origins (1)
56:4
Osama (10)
8:21;134:21;137:8;
139:10;153:1,13;154:5,7;
158:6;165:20
others (5)
47:6;79:1;130:10;139:7;
143:13
other's (1)
133:9
Otherwise (6)
17:11;75:15;100:11;
106:21;107:8;132:21
out (20)
7:6;8:2;39:20;57:7;
58:12;69:16;85:1;88:20;
108:18;115:5,8,20;116:18;
117:16;119:6;144:19;
145:2;148:2;159:8;163:12
outcome (1)
163:15
outlets (1)
144:11
outlines (1)
2:13
Outlook (13)
110:10;114:6,17;115:1,6,
7,10,10,16,21;116:5,7;
118:9
outside (3)
50:18;75:15;82:13
over (37)
5:20;11:7;20:12;35:2;
42:18,18;45:20;47:21;
61:20;69:18;70:18;71:1;
77:12;83:16;84:2;87:4;
89:8,8,16;90:9,12,21;95:19;
96:7,11;121:15,15;122:5;
123:10;125:13;132:1,14;
136:2;138:9;161:17;
163:17;165:12
Overall (2)
35:16;122:10
OVERGAARD (1)
3:6
over-redundancies (1)
111:2
oversight (2)
30:4;143:5
overt (2)
148:14;163:4
overwhelming (3)
45:16;130:2,12
own (24)
4:10;20:10;41:12;42:11;
44:1;45:7;47:3,17;83:21;
109:17;119:9;131:18;
136:12,13;139:8;140:18;
142:6;147:8,11;156:6;
162:9;164:20;166:5,7
owned (1)
97:5
ownership (2)
68:17;95:3

P

package (1)
117:11
packaged (1)
91:11
Packnett (1)
34:1
page (43)
21:2;30:15;32:7;34:8;
41:8;45:7;47:20;53:15,17;
61:21;63:14;65:7,12;67:1;
82:7,7,19;83:5,8,19;84:16;
86:15;87:10,18;88:13;
103:21;106:11,15;114:14;
145:12,20,20;147:18;148:4,
5;161:13;162:13;163:8,9;
164:11,15;166:14,15
pages (10)
29:12;31:12;66:10,11;
73:3;106:7,7,13;115:5;
159:5
paid (4)
25:4,10;26:12,18
Pakistan (2)
153:3;158:10
papers (1)
66:14
Paragraph (6)
41:12,16;64:19;72:6;
106:9;109:20
paragraphs (4)

72:5;74:19;75:13,14
parochial (1)
148:9
part (9)
8:15;11:6,16;58:8;75:10;
99:20;100:3;152:20;165:18
partial (1)
56:3
participated (1)
41:4
particular (6)
20:1;48:10;100:13;129:4;
138:7;158:14
particularly (2)
10:19;147:5
parties (3)
4:3;59:4;125:9
pass (2)
56:13;113:11
passed (1)
140:20
password (14)
13:15;14:2;40:17;45:9;
49:10,11;54:2,9;57:3,5,17;
58:2,8,12
passwords (4)
49:8,15;53:12;57:3
past (3)
30:2;132:14;138:9
paste (2)
88:11,15
pasted (3)
88:15,19;89:4
path (2)
19:11;85:21
pattern (1)
140:16
pause (1)
162:7
pay (15)
22:3;24:6,20;25:21;26:8;
68:9;70:13,18;94:19;95:12,
19;96:7;122:15;123:10;
124:15
PDF (1)
73:16
PE12 (1)
143:19
PE127 (1)
40:6
PE130 (1)
56:11
PE145 (1)
115:13
PE42 (2)
18:3,5
PE47 (1)
111:11
PE52 (1)
137:11
PE92 (1)
13:18
PE99 (1)
144:3
penetrate (1)
120:5
penetrated (1)
120:8
penetrating (1)
161:14
penetration (1)
98:13
Peninsula (11)
134:13,18;135:8,13;
142:3;146:18;152:10,17;
159:1,12;166:2
people (6)
41:21;49:15;148:8,16;
151:11;164:13
people's (1)
47:8
per (13)
11:13;25:10;26:18;69:15,
16;70:3;96:7;122:1,2,4;
130:16,16,17
percent (5)
25:7,13;26:16,20;162:10
perception (1)
156:21
perform (2)
140:2;159:15
performed (1)
47:5
perhaps (1)
19:1
period (3)
5:20;11:7;87:5
permanently (1)
117:17
permission (3)
101:15;118:21;119:1
permissions (1)
118:8
permitted (2)
2:4,7
persistence (1)
94:1
person (11)
20:2,2,4;42:6;48:10;
50:21;61:8;69:12;110:8;
120:17;148:17
personal (44)
15:4,15;16:3,13,17;17:2,
5;20:12;21:7,14;38:5;
39:21;42:11;47:4;51:13,16,
20;56:17;67:15,20;68:21;
69:1;74:9;76:3;83:21;
84:12,12;90:16;92:16;94:4,
10;99:14;109:17;117:2,10;
119:9,12,13,15;124:2,5,8,
13;163:19
personnel (4)
21:11;67:17;94:7;124:11
persons (2)
10:1;112:13
pertaining (8)
24:9;26:2;60:17;70:15;
81:2;95:15;122:21;142:7
PFC (380)
1:6;4:10,16;6:15;7:12;
8:8;9:3;10:6,11,13,17,18;
11:21;12:14,20;13:5,8,11;
14:3,18;15:1,3,8,10,11,15,
20,21;16:2,5,11,16;17:7,16;
18:1,5,14;19:9;20:8,9,16,
20;21:6,13,16,19;22:9;23:6,
15;27:6,11;28:2,5;30:6,18;
31:13;32:3,6,14;33:5,8,10,
12,18,21;34:16,21;35:1;
37:19;38:2,8,10,14,20;39:2,
8,12,16;40:12,14,17,21;
41:3,8,9,18;42:20;43:8,13,
17;44:1,2,4,15,18;45:16;
46:2,6,7,12,20;47:2,7,13,21;
48:6,21;49:3;50:5;51:8,16,
21;52:3,15,19;53:1,8,11,18;
54:1,14,17;55:10;56:1,6,16,
20;57:6,11,15;58:9,12;
59:13,19;60:7;62:1,9,11,20;
63:2,9,17,20;64:2,5,7,21;
65:8,13,15,18,21;66:3,7,12,
14;67:14,19,21;68:3,16,20;
69:5,18;71:4,7;72:1,14;
73:10;75:19;76:1,6,20;77:3,
3,4,6,8,11;81:7,11,14,20;
82:1;83:14,20;84:1,8,11,18,
19;85:3,7,10,14,16;86:7,9,
9;87:1,8,15,16;88:2,9,17;
89:1,4,12,15;90:3,8,13,15;
91:3,8,19;92:7,16,20;93:10,
17,17;94:4,8,11,14;95:1;
96:14;97:8,15;99:4;101:12,
13;102:5,10,13;103:6,19;
104:3,4,9,12,14,17,19;
105:1,15,19;106:3;107:1,4;
108:11;109:2,8,12,20;
111:19;113:5,8,14,17,21;
114:3;115:20;116:17;
117:1,5,15;118:14,17,21;
119:6,15;120:1,4,7,10;
121:17;122:7,11;123:16;
124:1,7,12;126:5,14;127:1,
5,14,18;129:13,13,17,20;
130:2,6,14;131:3,13,21;
132:5,16,20;133:2,18;
134:2;135:11,12,17;136:1,
4,6,16;137:1;138:5,18;
139:2,12;140:1,15,18;
141:6,18;142:4,13,17;
143:9,11,19,20;144:3,17;
145:6;146:4,13,18,21;
147:6,13;148:1,6,15,21;
149:2;150:6,10,11,15;
151:4,9;152:3,8;153:18;
154:10,16;155:1,21;156:9;
157:9,14;158:2,11,17;
159:13,15;160:1,10,20;
161:3,12;162:7,14;163:9,
15;164:21;165:7,15;166:7,
10
phishers (1)
119:20
phishing (3)
98:16;120:2,3
phone (1)
112:18
photo (1)
19:19
physical (2)
112:20;162:10
physically (1)
84:1
PI (2)
124:3,4
picture (4)
19:13,17;20:2,4
piece (2)
37:4;54:4
pieces (4)
46:21;49:17;117:21;
121:2
piecing (1)
137:17
PII (2)
78:18;137:19
pilot (2)
35:10;36:7
pilots (1)
35:13
place (8)
2:5;5:19;6:2;48:1;58:10;
82:13;88:4,5
placed (6)
68:20;74:9;85:14;124:1,
5;164:9
placement (1)
36:2
places (1)
157:1
plagued (1)
65:21
plain (3)
49:10;57:3;58:15
planning (1)
30:13
plans (1)
95:15
playback (1)
155:14
please (4)
24:15;41:9;56:15;108:21
plot (1)
6:2
plus (2)
89:3;161:2
pm (3)
1:16;46:12;167:9
point (11)
7:21;27:1;37:6,7,8;39:7;
47:12,13;67:2;71:21;83:11
pointed (2)
151:8;159:8

pointing (1)
83:12
points (1)
29:9
pole (1)
54:14
policies (2)
131:8;149:12
policy (6)
34:4;76:18;78:1,5;79:7;
129:7
politically (1)
60:3
populates (1)
110:7
portal (1)
143:17
portion (12)
10:7,9;53:8,10;57:13;
71:14,16;72:13;104:12;
111:21;112:2;122:10
portions (5)
14:7;20:18;21:3;37:12;
39:5
posed (4)
29:1,4;144:18;160:20
poses (1)
145:21
position (2)
71:5;106:21
positions (2)
112:15;123:8
positive (1)
157:1
possessed (2)
90:16;99:9
possessing (1)
147:11
possession (12)
22:4,8;29:19;68:10,13;
94:20;95:3;124:16;136:21;
141:16;152:11;154:12
possessions (1)
17:17
possible (2)
91:4;108:21
possibly (1)
140:21
post (4)
29:20;44:2;143:4;150:18
posted (13)
30:8;31:9;35:4;75:11;
76:4;79:9;137:15;138:1;
142:11;153:7,10;160:16,18
posting (2)
30:19;148:21
posts (3)
30:2;77:17;146:14
potential (11)
29:10,16;36:5;58:16;
111:2;112:15;115:5;
138:13;142:18;143:2;158:1
potentially (3)
52:5;112:4,19
Potomac (2)
15:1,21
power (1)
148:14
PowerPoint (2)
137:6;139:7
practice (1)
107:2
precise (2)
114:8;163:15
precisely (5)
22:4;68:10;94:20;117:5;
124:16
predeployment (2)
151:3,7
pre-deployment (1)
140:4
predict (1)
140:12
predictive (3)
6:12;28:15;140:11
PreFetch (3)
85:17;86:4,6
prejudice (1)
133:21
prejudicial (1)
131:13
prepare (2)
84:10;88:10
present (9)
4:3,4;59:4,5;72:15;
125:10,10;154:2;155:5
presented (3)
12:16;71:12;100:14
preserved (1)
35:21
press (2)
33:16;40:19
presume (2)
143:6,7
presumed (1)
30:6
pretty (1)
46:21
prevent (1)
49:14
previous (5)
7:1;38:10;39:8;61:10;
161:10
previously (3)
117:20;123:17;127:8
price (2)
25:10;26:17
primarily (2)
35:8;71:13
primary (1)
52:9
principle (1)
148:8
print (6)
54:3;72:5;82:10;83:11;
84:5;86:21
printed (2)
91:14,18
prior (6)
7:12;15:7,9;17:14;36:5;
132:11
priorities (2)
42:9;80:12
privacy (1)
44:11
Private (4)
10:20;11:9;13:14;119:2
privileges (4)
50:5;52:11;99:4,7
probably (3)
22:11;58:19;106:5
problems (1)
151:17
procedures (4)
7:5;24:10;26:3;36:13
proceed (1)
125:11
proceedings (3)
2:5,9;4:1
process (12)
8:16;28:8;55:5,15;87:2,2;
89:2;109:11;113:19;
115:19;117:5;156:8
produce (1)
2:9
produced (2)
32:2;129:5
producer (1)
70:3
product (6)
28:16;69:9;110:7;136:7;
140:2;141:6
products (1)
28:9
professing (1)
41:17
professional (1)
7:20
professionals (1)
69:10
profile (2)
48:14;73:14
program (22)
9:10;28:11;51:3;59:18;
63:21;65:1,4,13,14;69:4;
85:18;89:2,8;90:16;96:19;
97:15,17;99:19;100:1;
101:19;102:15;115:16
programming (2)
114:14;115:17
programs (7)
48:14;64:18;96:18;
100:15;101:8;102:18;
115:18
progressive (1)
163:5
prohibited (4)
64:12;100:17,21;102:10
pro-insurgent (1)
141:11
projections (1)
55:19
prompt (3)
65:10;89:19;101:19
proof (1)
71:12
propaganda (3)
141:15;157:5;159:1
proper (2)
97:6;120:21
properly (3)
31:19;74:16;107:18
Prosecution (103)
4:14;13:2;15:13,16,18;
16:3,4,18,18;19:7,13;27:20,
21;29:12;30:16;31:15,20;
32:1,13,21;40:5;41:7;43:3,
5;45:7;46:17,18;47:20;
51:14,15;53:16;54:7,12;
55:20;62:8,17,19;63:5,14,
19;64:2;65:6;66:18,20;
72:5,7,10,17,21;73:10,18;
74:8,13,18;75:6,12,13,17;
78:6,14;79:12;84:15,19;
85:6;86:5;87:13;89:21;
90:3,11;91:13,19;92:2,9,12;
104:7,11,17,18;105:13;
111:7,9,13;113:20;114:10,
18;115:2,13;116:13;
134:20;135:2;137:6;139:6,
8,13;141:4;142:15;145:7;
153:12,21;154:7,13,19;
155:3
Prosecution's (1)
125:12
prosecutor (1)
67:9
protect (14)
6:10,17;19:18,19;21:21;
34:4;37:21;49:7;57:17;
68:6;94:16;138:16;150:3;
162:4
protected (11)
13:15;18:17,21;19:1,5;
36:2;37:5;45:6;53:4;119:7;
124:3
protecting (2)
37:15;150:12
protection (4)
29:10;49:21;50:11;
142:19
protections (1)
57:19
protocol (1)
57:16
protocols (1)
57:13
proud (1)
19:9
prove (3)
33:8;130:6,12
proved (2)

131:13;135:21
proven (2)
118:2;157:6
proves (1)
139:12
provide (6)
5:18;29:14;80:8;143:1, 16;165:9
provided (12)
10:13;14:3;20:21;28:1; 53:19;56:6;60:6;127:2,8; 155:21;161:6,12
provides (9)
22:4;49:21;56:2;68:10; 94:20;110:13,17;112:9; 124:17
providing (3)
21:3;80:3;141:21
province (1)
103:10
public (25)
22:16;36:5,17;37:7; 41:18;42:7;44:13;67:12; 108:6;126:8,16;127:3,12; 131:2,9;136:3;142:1; 145:16;148:3;149:13,15,15, 19;150:1,12
publication (5)
21:18;22:6;68:2,12; 154:14
publications (1)
141:7
publicly (4)
34:16;44:10;67:2;145:14
published (17)
60:1;67:1;68:4,16;72:4; 77:4;88:14;92:18;93:6; 94:15;95:1;109:8;127:19; 130:7;145:16;158:21;159:4
pull (1)
6:1
pulled (3)
13:9,11;115:8
Pulling (1)
11:18
purely (1)
8:12
purported (8)
36:21;66:18;79:9;92:18; 93:7,8,20;128:19
purpose (8)
28:21;102:20,20;110:1; 114:2;118:16;123:19;155:7
purposes (6)
2:8,15;30:13;118:4; 134:9;164:20
push (1)
11:13
put (7)
5:12;11:11;42:12;46:21; 82:13;88:4;150:15
putting (1)
137:3

Q

quarter (3)
35:10;84:2;89:16
query (1)
88:13
quest (2)
38:5;39:14
quickly (4)
57:4;89:2;113:14,17
quotation (1)
41:11
quote (14)
4:11;41:10,16;114:16,17; 115:9;143:13,15;145:12,13; 148:2,4,6;149:17

R

rack (3)
25:21;26:9,9
raid (1)
154:8
raided (1)
153:3
rainbow (8)
46:13,19,20;48:4;56:2, 21;57:1,7
ran (2)
86:1,7
rank (3)
112:3;121:21;122:1
ranking (2)
69:12;121:18
ranks (2)
131:19;162:19
rapid (1)
30:11
rapidly (1)
89:8
rate (2)
66:1;122:4
rather (4)
41:19;87:18;148:17; 163:20
reach (1)
116:18
reached (2)
144:19;145:2
reaction (7)
40:14;42:18;43:16;45:21; 75:20;105:18;127:11
read (13)
18:2;19:14,17;55:17; 76:7;83:2;142:9,11;143:7, 20;145:4;146:4;152:7
reader (1)
143:6
readers (1)
30:10
readily (1)
109:5
reading (6)
33:13;137:15;138:4; 142:6;146:7,12
ready (1)
93:11
real (1)
165:10
reality (1)
39:10
realized (1)
39:8
realtime (1)
8:16
reaping (1)
81:21
Rear (3)
61:4,9;107:16
reason (17)
24:13,15;25:2;26:6,11; 55:9;70:16,20;76:9;95:17, 20;119:4;120:15,15;123:2, 12;160:8
reasonable (4)
17:6;136:1;141:19;166:8
reasonably (1)
75:3
rebuttal (1)
126:2
recall (3)
52:1;77:5;118:3
recalled (1)
151:21
receive (5)
34:18;56:7;129:19; 136:19;143:5
received (16)
9:1;30:3;41:2;96:4; 137:7;139:11;146:14; 152:16;153:14;156:18; 158:7,8,9;164:2;165:20; 167:2
receives (1)
129:2
receiving (2)
33:17,20
Recent (1)
29:13
recess (11)
58:18,21;59:2;124:20; 125:4,6,7,13,17;167:5,8
recessed (4)
4:4;59:5;125:10;167:9
reckless (1)
127:5
recklessness (2)
130:13;133:2
recognition (1)
164:16
recognized (3)
131:10;158:2;159:13
recognizing (2)
21:4;164:12
recollect (1)
93:4
recommendation (1)
60:12
recommends (1)
124:20
record (6)
4:3;59:4;73:7;91:1; 125:9;133:1
recorded (3)
13:7;66:5;75:12
recording (1)
2:7
records (30)
21:6,8,14,17,20;26:8,18; 59:17;67:16,20;68:18,21; 69:1,2,7;70:18;94:3,5,6,9; 95:4,12,12,19;113:4;114:2; 116:18;123:11;124:9;129:5
recover (1)
17:1
recovered (3)
17:13;113:21;116:9
recruiting (1)
138:6
recruitment (2)
154:20;157:13
recycle (1)
117:17
red (1)
36:19
redactions (1)
92:19
redeploy (1)
132:9
redirect (1)
6:7
rednecks (1)
166:13
reduction (1)
151:19
reference (2)
71:20;135:4
referenced (2)
27:4;111:14
refers (1)
71:14
reflect (2)
4:3;59:4
reflected (4)
32:21;73:18;74:13;125:9
reflects (1)
28:17
refocusing (1)
113:18
reform (1)
150:11
refrain (1)
47:10
regard (4)
28:12;35:7,19;100:2
regarding (6)
39:4;42:8;60:17;79:5; 134:12;141:10

region (1)
38:9
regions (1)
158:9
regulates (1)
100:19
regulation (3)
57:20;101:3;124:4
reinstalled (1)
15:12
reintroduce (1)
91:5
reintroduced (1)
93:18
relate (1)
107:10
related (12)
10:19;42:21;46:3;76:18;
83:2;84:21;96:7;104:1;
105:8;114:14;116:10;
136:10
relates (2)
22:19;34:12
relating (1)
129:4
relations (5)
75:1,5;79:5,6;128:21
release (22)
23:12;29:4,6;31:4;33:16,
17;35:1;36:5,9;38:3;41:18;
45:5;75:20;77:13;94:13;
105:20;112:18;127:7,16;
141:21;142:21;164:2
released (42)
4:11;7:18;19:6;21:20;
30:2;34:16;37:7;38:7,11;
39:9,13;40:16;41:5;44:13,
14;45:4,21;66:17;67:2;
75:8,15;93:8,21;105:12;
106:3;126:8,16;127:2,9,12,
14,21;128:3,5,11,19;134:6;
136:5;153:16;154:10,20;
157:3
releases (1)
29:13
releasing (3)
128:16;146:11;162:20
relevance (1)
113:16
relevant (1)
148:10
relied (2)
6:12;120:11
relies (2)
133:18;148:14
relocate (4)
70:7;72:1;95:6;122:17
relocated (1)
23:16
rely (1)
133:8
remainder (1)
125:11
remaining (3)
71:16;93:18;103:21
remedy (1)
84:9
remember (2)
64:11,15
remembered (1)
151:18
reminder (1)
73:1
remnant (2)
17:3,11
removed (3)
19:5;108:18;109:5
removing (3)
18:17;124:3;141:2
render (1)
112:19
repeated (2)
142:6;152:5
repeatedly (5)
34:9,10;59:14;126:18;
136:11
repercussions (1)
146:3
report (31)
4:19;9:15;16:16,20;
27:18;28:1,10,12,19;29:3,
21;30:5;31:2,4,11,19;32:9,
15;33:8;34:12;126:21;
128:1,1;129:9;142:12;
144:5;145:5,7,10,11,20
reporter (4)
2:3,3,14,17
reporting (7)
2:13;9:8;67:12;80:10;
143:10;144:12;152:1
reports (17)
8:3,4,6;19:4;22:13;34:2;
43:20;126:19;128:9,13,20;
129:3;136:10;142:10;
146:5,6;156:6
report's (1)
29:8
reposed (1)
138:15
repository (2)
131:8;149:11
represented (1)
142:18
represents (1)
29:10
reputation (1)
146:9
request (4)
27:5;42:15;71:3;72:1
requesting (2)
97:16;153:6
requests (4)
27:8;70:7;95:5;122:17
require (1)
27:3
required (4)
11:19;87:3;107:7;140:2
requirement (1)
82:14
requirements (1)
132:7
requires (1)
130:5
rescue (4)
51:2,9,12;57:19
research (5)
28:19;46:20;65:13;
127:10;136:10
researched (3)
38:10;59:13;115:20
researching (2)
39:12;161:8
reserved (1)
99:3
resided (1)
80:13
resorted (1)
50:5
resource (3)
7:17;56:2;77:20
resources (5)
21:21;42:9;68:6;94:16;
110:4
respect (1)
106:12
responded (1)
56:12
response (2)
5:11;37:10
responses (3)
4:21;24:11;26:4
responsibility (3)
81:6;99:15;138:12
responsible (2)
5:9;7:9
responsive (1)
96:4
rest (2)
81:3;120:9
restrictions (3)
82:13;88:4;91:2
result (4)
77:6;80:5;132:20;147:10
resulted (1)
103:11
results (6)
81:19;86:16;87:19;
114:14;115:4,12
Retired (2)
67:7;107:12
retrieve (4)
27:5;72:2;123:14;134:7
retrieved (1)
27:10
retrieves (1)
96:12
return (2)
83:8;114:17
returned (3)
16:1;103:20;115:12
returning (3)
17:16;39:16;81:17
Reuters (1)
42:21
reveal (2)
7:19;79:4
revealed (3)
28:20;45:3;132:5
revealing (1)
141:2
reveals (3)
4:12;72:8;123:5
revelation (1)
148:12
reveling (1)
105:17
reverse (1)
54:1
review (3)
16:11;30:7;160:17
reviewed (4)
7:2;36:4;59:15;126:18
reviewing (1)
166:4
Reykjavik (4)
40:2;60:5;76:21;81:19
right (13)
11:12;33:6;54:19,20;
56:14;62:12,14;84:5;94:3;
111:16;125:1;133:13;167:4
rights (3)
68:17;79:1;95:3
RIP/TOA (1)
33:6
rippling (1)
105:19
risk (3)
79:1;124:3;131:4
road (1)
6:2
ROE (1)
143:14
role (1)
43:18
room (4)
2:5;42:4;44:19;113:7
rooms (1)
102:2
rotations (1)
147:7
roughly (1)
160:13
route (3)
5:20;6:7;156:10
Royer (13)
98:3,8,15,17;101:17;
102:1;110:20;112:5;113:3;
118:3;120:14;121:12,18
ruling (1)
134:15
run (11)
50:15;64:3;85:2,16;86:3,

9,10;89:7;96:19;101:19,21
running (4)
64:6;65:5,20;88:9
runs (1)
85:19
Russia (2)
149:18;150:16

S

S2 (4)
80:17;111:6;113:6;143:13
sad (1)
132:2
Sadtler (1)
102:4
safe (2)
48:1;119:7
safeguard (2)
8:3;137:2
safekeeping (1)
15:5
safest (1)
156:10
salary (2)
69:15;122:6
SAM (15)
49:19,19;50:1,12,16;52:5;53:20;54:18,19,21;55:6,12;56:3;57:14;58:7
same (31)
12:9;14:2,13;17:21;18:10;19:14,15;36:8;40:7;52:2;55:15;63:10;74:3;81:8;90:12;92:15;105:21;106:15;108:10,16;110:21;116:17;117:5,19;131:1,11;132:2;153:8;154:20;156:8;159:15
sanitized (1)
36:4
sat (2)
18:21;19:2
save (11)
8:16;62:13;82:11;83:1,11;84:5;85:18;86:21;87:19;116:5,6
saved (2)
73:12;76:2
savvy (1)
163:6
saw (8)
37:14;38:10,14;43:18;77:7;105:19;109:2;112:14
saying (1)
43:19
scale (1)
20:8
schemes (1)
119:21
Schmidle (2)
41:8;43:19
SCIF (3)
45:18;97:18;108:18
scope (3)
132:5;147:14,16
Scott (1)
44:11
scrape (2)
87:11;102:21
scraped (1)
68:19
scrapes (1)
98:18
screen (3)
11:13;18:4;102:6
script (2)
90:16,21
scrolled (1)
106:15
scrolling (1)
61:20
SD (14)
4:15;13:17,20;14:19,21;15:5,5;17:17;18:1;19:16;20:6,9,12;21:14
Sean (1)
110:18
search (35)
43:2,6,8,8;46:13,19;47:10;48:4,16;56:21;72:8;83:7,7;84:4,21;85:1,4;86:15,15;87:19;96:2,3;105:14;114:13,16,20;115:1,4,4,9,12;116:19;118:8;144:4;145:8
searchable (3)
131:9;149:12,14
searched (12)
34:9;46:6;60:8;72:8;76:1;82:18;84:20;96:7;105:15;109:9,11;160:11
searches (2)
42:21;160:13
searching (3)
64:2;84:18;142:6
Second (9)
49:16;56:14;58:7;73:13;88:17;115:9;127:4;144:2;153:15
secondly (1)
125:19
seconds (2)
46:16;74:4
secret (17)
22:11;23:3,11;31:11,20;37:3;61:7;66:21;79:16;101:15;106:5,7,13,14,16;107:15,18
secrets (2)
138:16;163:4
section (2)
44:12;45:9
security (25)
23:2,12;31:5;50:9;52:21,21;53:2;57:12;58:1,2,10;61:6;79:15;80:19;107:14;112:13,20;113:12;131:18;132:8;144:16,18;162:11,12;164:10
seeing (1)
132:13
seek (12)
24:5,8;25:20;26:1;41:18;70:12,14;95:11,14;113:4;122:14,21
seeking (1)
145:3
seem (1)
161:20
seems (1)
12:13
selecting (1)
116:6
self (1)
45:2
self-admitted (1)
146:9
self-described (1)
144:8
self-executable (1)
100:6
self-help (1)
84:9
self-initiated (1)
28:9
send (1)
120:17
senior (2)
28:14;36:7
sense (3)
2:16;139:18;166:5
sensitive (11)
29:14,19;30:8;36:6;78:3;79:4;119:15;124:4;137:3;160:18;162:4
sensitivity (3)
37:15;38:1;112:14
sent (3)
77:17;80:15;143:11
separate (1)
96:5
separately (1)
9:11
September (1)
79:21
Sergeant (10)
6:18;7:11;102:4;113:5;116:11,15;118:20;151:14,15,17
series (2)
78:15;79:13
serious (6)
23:2;31:5;61:6;75:4;79:14;107:14
serve (1)
59:10
server (12)
12:12,21;32:20,21;87:11,12,20;102:21;104:18;114:7;120:17,18
servers (5)
12:6,8,11;13:5;90:2
serves (2)
30:18;159:1
service (14)
9:18,20;25:3,6,12;26:12,15,20;35:17;71:2;120:11;121:8;131:14;133:21
services (20)
22:3;24:4,8;25:19;26:1;29:15;68:9;70:5,11,14;94:19;95:10,14;96:11;122:14,21;123:5,10;124:15;143:1
session (3)
71:12;72:19;151:7
set (11)
25:1;26:10;59:9;70:20;77:8;95:20;103:2;108:18;110:3;113:18;123:11
sets (1)
4:7
setting (1)
47:9
seven (2)
10:5;16:8
several (5)
75:19;131:5;149:9;153:4;158:4
severed (2)
108:12,17
share (6)
12:9;38:17;43:15;61:15;80:6;100:9
shared (1)
81:8
SharePoint (5)
104:8,18,19;106:11;114:6
sharing (3)
80:2,11;82:15
Shaver (51)
12:19;13:16,19;14:14;17:1;32:3;48:8;49:6,14;50:13,20;51:4,7;52:2,4;53:7;54:5,15,16;55:14;56:21;58:4;62:11,14;63:6,10;64:1,5,16,21;65:8;72:13,17;73:4,19;83:4,17;84:21;85:9,12,21;87:14,16;88:14,21;89:6,9;93:14;101:20;104:2,21
sheet (2)
125:15,18
shift (3)
56:16,17;97:4
shoe (2)
39:21;40:8
shook (1)
132:17

shop (3)
80:17;113:6;143:13
short (3)
48:19;87:5;112:17
shortest (1)
91:4
shortly (1)
109:8
shoulder (1)
151:8
show (9)
13:4;16:5;24:10;26:3;62:7;72:18;75:9;92:14;137:6
showed (9)
36:17;63:12;66:20;91:10;92:9;136:6;141:7;153:17;154:21
showing (8)
54:17;104:8,13,19,20;108:1;128:20;165:15
Showman (5)
38:15;151:3,6,13,21
shown (2)
40:3;85:6
shows (25)
15:6;32:6;35:13;40:6;51:20;54:21;59:21;62:9,20;63:2;64:2;76:8;84:19;86:6;89:21;90:3,11;91:19;92:2,12,13;104:17;135:18;150:6;164:21
shy (1)
56:18
side (4)
54:19;55:3,7;56:14
SIGACT (11)
4:18,19;5:4,6;6:19;13:9;16:21;17:8;22:12;26:14;129:10
SIGACTS (74)
4:10,15,17,20;5:12,14,16;6:1,9,15,16;7:3,8,13,14,15,16;9:2,21;10:8,10,12,14,19;11:2,3,6,8,15,18;12:14;13:9,12;14:8,19;15:4;17:2,3,12,19;18:1,11,20;19:17;20:7;21:1,9;22:6;23:10,11;24:1,5,6,21;25:5,7,10,16,20,21;26:9,16,18;39:5;43:21;128:6,12;134:4;140:20;152:14,21;153:9;156:2;159:18
sight (1)
58:15
signed (2)
107:5;138:11
significance (3)
18:7,12;28:12
significant (17)
4:12,20;9:14;18:13,16;21:21;22:5;68:5,11;94:16,21;101:2;124:17;128:10,13;138:1;141:1
signified (1)
63:7
signing (1)
151:18
signs (1)
155:15
similar (7)
25:5;26:13;37:13;73:17;82:21;140:16;151:11
simple (4)
65:3;86:12;115:17;150:5
simpler (1)
90:20
Simply (2)
5:12;150:15
single (9)
17:3;31:4;76:20;82:11,11;89:15;91:20;101:10;164:9
SIP (1)
81:12
SIPR (1)
81:12
SIPRNET (70)
7:15,16;10:6;11:20;12:15;19:6;21:12;22:15;31:7;32:11;33:5;36:3;38:17,17;39:19;42:15;43:9;44:7;45:17;46:3,6,12;47:15,18;48:6,9,16;49:1;50:7;52:19;53:6,9,20;56:8,20;57:6,21;58:13;61:15,16;72:9,14;76:2;80:4,6,9,14;85:15;92:12,15;100:12;102:15;103:16;104:6,13,15;106:11;107:3;108:11,17;109:6;113:11;129:6;139:2;143:19;161:5;163:14,18;164:1;165:13
sisters (1)
119:16
sit (1)
19:18
sites (7)
69:4;73:8;98:18;138:8;141:11;157:12;162:6
sitting (1)
102:7
six (5)
11:2;57:8;161:3,5,8
SJ (1)
103:20
skilled (1)
150:18
skills (2)
10:21;42:11
slash (3)
143:17,17,18
sleep (1)
121:16
slice (2)
85:18,19
slide (2)
137:6,11
slow (1)
62:15
smart (1)
81:15
smil (1)
143:18
smiling (2)
19:15,19
snapshot (1)
155:14
social (1)
98:16
society (1)
139:19
software (6)
55:15;64:8;97:1;99:1,3,7
sold (1)
149:18
soldier (19)
33:6;42:8,10;100:13;113:10;121:11,16,21;133:5,6,8,12;141:8;148:18,18;164:6,7,19;166:17
soldiers (22)
6:10,17;7:1,6;19:20;38:15;64:12;80:16;81:10;96:17;97:18;99:19;113:2;121:18;124:2;132:11;137:14;138:2;150:3;155:13;162:6;166:12
sole (1)
166:17
somehow (1)
36:17
someone (3)
52:13;101:17;161:14
soon (1)
39:9
sorry (2)
45:12;98:3
sort (3)
35:21;50:6;150:13
sorting (1)
161:18
sought (1)
160:2
source (11)
10:3;18:20;19:2;37:1;40:20;42:18;43:9,11;75:18,20;138:20
sources (13)
6:17;10:2;28:11;37:15;45:6;53:13;75:1;76:18;78:18;79:1,6;134:11,14
South (1)
81:2
SOUTHCOM (5)
60:12;65:15;70:13,18;129:10
Southeast (2)
80:20;81:1
souvenir (1)
43:16
space (3)
17:9;117:4,15
span (1)
79:9
spark (2)
148:17;150:10
spear (4)
98:16;119:20;120:2,3
Special (61)
12:19;13:16,19;14:14,21;16:21;28:9;32:2;48:8;49:6,14;50:13,20;51:4,7;52:1,4;53:7;54:5,14,16;55:14;56:21;58:4;62:11,14;63:6,10;64:1,5,16,21;65:7;72:12,17;73:4,19;79:8;83:4,17;84:20;85:9,12,20;87:14,16;88:13,21;89:6,9;93:14;101:20;104:2,21;109:7;114:12;115:14;116:2,9,15;128:18
specialist (6)
69:13,14;111:5;121:19;122:1,6
specific (15)
12:3;28:15;44:14;71:14;72:13;83:9;88:9;95:16;96:3;122:21;140:6;147:6;152:10;156:4;162:3
specifically (29)
16:4;21:19;24:3;25:18;29:3;30:20;34:13;51:9,16;53:1;57:16,17;64:13;68:3;71:20;74:20;80:8;94:14;99:17;105:14;107:5;134:12;135:10;142:2;148:6;152:13;159:8;160:2;166:6
specification (31)
27:15,17;34:20;45:10,12;47:1;59:8,10,11;64:20;71:3,9;76:15;103:4,4;106:4;107:9;108:8,8,9,13,15;109:14,16,19;126:4,10,11,12;130:5;131:15
Specifications (6)
4:8;22:10,19;76:14;103:2;166:9
specified (1)
99:3
speed (1)
53:11
spending (1)
166:6
spent (3)
63:18;69:21;90:8
splash (2)
40:13;41:2
splits (1)
49:17
spot (1)

164:10
spreadsheet (2)
14:13;89:5
staff (4)
100:9;116:11,15;131:21
staggering (1)
90:1
stand (2)
95:7;111:15
stands (2)
115:14;151:5
start (2)
19:11;126:1
started (4)
45:16;62:12;93:4;113:6
Starting (6)
10:21;45:18;93:11,19;
105:11;161:4
starts (1)
133:15
state (36)
36:21;75:14;77:13,16,17;
78:16;79:18;80:3,9;82:7;
84:13;86:11;87:11,21;90:2,
4;92:18;103:1;107:6;
128:16;134:4;148:13;
149:7,20;152:14;153:7;
154:3,9,12,21;155:4;
157:15,20;159:19;163:3;
164:8
stated (5)
20:20;34:7;92:20;101:9;
158:3
statements (2)
136:12;147:12
STATES (103)
1:2,4;9:6;10:4;18:16;
21:21;22:5,7,15,20;24:9;
26:2;27:8,10;28:3,4;29:2;
30:14;33:8;35:2;36:19;
44:17;46:1;49:2;57:10;
60:7,15,17;61:3;68:5,11,13;
69:13;70:6;71:8,12,13,19,
21;75:5,16;76:10,17;78:1,4;
94:16,21;95:5,15;96:12;
102:9,16;103:14;105:5;
107:10;108:3;119:7;120:3;
122:17;123:7,8,13;124:17,
19;129:5;130:6;131:12;
132:13;134:10,12,17,19;
135:9,14,21;136:18,20;
137:19;143:3;144:12;
146:10;148:6,18;150:2,13;
151:4;153:2;154:5,8;
155:19;156:1,7;157:8;
159:7,16;161:7;164:4;
165:7,8,16;166:1,3,18
States' (2)
68:17;95:3
stating (1)
143:13
stationed (1)
11:21
status (3)
9:16;66:9;107:7
statutory (3)
24:2;25:17;121:5
stay (3)
71:4;133:7;161:20
stayed (1)
15:2
steal (3)
10:7;82:2;114:4
stealing (3)
66:12;69:7;81:20
stellar (1)
133:1
step (1)
117:16
steps (7)
5:11;45:1;57:18;88:9;
117:19;163:16;167:1
stick (1)
45:3
still (2)
16:14;102:7
stipulation (8)
31:16;134:21;135:3,6;
153:1,11,20;154:6
stole (8)
45:19;59:19;66:16;69:18;
77:4;121:17;122:8,11
stolen (2)
78:17;109:13
stood (1)
19:15
stop (1)
59:20
storage (2)
100:17;101:3
store (3)
7:15;48:11,13
stored (11)
13:14;14:8;18:2;21:10;
61:14,19;67:16;94:6;
103:14;124:9;129:6
storing (2)
49:9,17
straight (2)
87:18;121:15
strategic (1)
95:15
strategies (2)
24:11;26:4
strength (1)
123:5
strengths (1)
140:9
structure (1)
112:16
study (2)
11:6;140:11
studying (1)
140:3
stumbling (1)
42:6
subexhibits (1)
78:8
subfolder (1)
103:17
subject (2)
39:13;77:2
submission (1)
69:4
submit (2)
109:1;145:15
subsequently (1)
32:16
substantially (2)
68:16;95:2
success (1)
66:1
successful (9)
5:7;8:2;63:11,12,16,17;
120:5;156:3,13
successfully (4)
16:11;53:8;57:12;63:9
suffering (1)
151:17
summary (7)
32:2;43:3;54:4,16;63:2;
67:11;104:12
superiors (1)
140:6
supervisor (2)
118:20;119:1
supplemented (1)
23:19
supply (4)
5:20;6:2,7;113:7
support (3)
81:10;107:21;165:14
supposed (1)
133:13
sure (2)
40:21;55:11
surrounding (1)
103:13
system (49)
9:8;15:13;19:6;21:10;
36:3;43:9;49:18,19;50:1,6,
8,12,15,16,19;51:2,11,12;
52:5,7,13,18,21;53:3;55:13;
58:1;61:16;64:6;67:17;
80:7;83:20;88:4;91:2;94:7;
98:13;99:10,13;100:20;
109:16,21;117:8,9;118:15,
18;119:8;120:11;124:4,9;
164:16
systematically (1)
165:12
systems (5)
47:15;108:2;110:2;120:9;
165:9

T

table (5)
8:11;27:6;29:5;56:2;57:7
tables (7)
46:13,19,20;48:5;56:21;
57:1,1
tactic (1)
141:15
tactical (12)
5:10,16;8:1,3,4,6,19;9:4;
128:9,13;155:11;160:3
tactics (4)
7:4;24:10;26:3;36:12
tale (1)
38:8
talk (3)
20:15;92:1;125:6
talked (3)
45:2;69:2;92:4
talking (3)
48:3;59:20;66:4
talks (1)
41:15
Tampa (4)
12:6,12,21;13:6
Tann (2)
77:15,19
tar (1)
13:15
target (3)
39:15;114:10;123:18
targeting (2)
29:17;30:13
Tasha (1)
110:18
task (5)
83:21;88:8;113:21;114:1,
3
tasked (1)
5:18
tasking (3)
20:14;84:12,13
tasks (1)
115:19
taught (6)
36:8;138:3;139:7,12;
157:10,10
T-drive (3)
100:9,12;101:5
teach (1)
7:18
teaches (1)
36:9
technical (2)
82:12;99:20
techniques (3)
7:5;24:10;36:13
technologically (1)
163:6
technology (3)
35:14,15;36:14
telling (3)
66:13;80:16;151:21
term (3)
86:15;89:1;115:4
terms (2)

2:15;46:6
terrorism (1)
129:7
terrorist (14)
8:9;29:15;34:14;60:19, 20;61:2;137:7;138:6,8,19; 143:2;153:21;154:20;157:6
terrorists (6)
60:18;61:1;139:14; 145:13;157:12,19
tester (1)
113:19
testified (164)
5:15,17;6:11,21;7:11,21, 21;9:10,21;10:18;12:5,19; 13:8,11,19;14:1,4,14,21; 15:20;16:10;22:2;23:1,9, 21;24:3,19;25:15,18;26:7; 28:7;32:13,18;35:20;36:7; 38:16,18;44:1,12;49:6; 50:13,20;51:4,7;53:7; 54:15;55:4;57:1;61:4,13, 18;62:11,14;63:6;64:1,5,12, 21;65:8;66:3;67:8;68:8; 69:8,11,19;70:10,17;73:4, 19;77:15,19;79:8,11,16; 80:1,7,13,15,18,21;81:4; 82:4,8,17,20;83:4,13,18; 84:21;85:9,12;87:6,14,16; 88:14;89:6,9,14;90:15; 93:14;94:18;95:9,18;96:1,6, 17,21;97:3,11,13,20;98:3,9, 15,20,21;99:2,6,8,12,14,16, 19;100:2,4;101:1,11,17,20; 102:1,5;104:2;105:1; 106:18;107:2,12,17,19; 109:7;110:6;113:3;114:13; 116:2,16;118:4,7;120:14; 121:7,12,18;122:13;123:9; 124:14;128:18;129:9; 131:16;132:4,12,19;133:4; 140:14;151:13,18;158:13
testimony (15)
2:16;9:13;31:17;64:15; 72:12,19;100:10;110:20; 116:13;124:1;135:6;151:6; 155:10;156:20;157:15
testing (1)
98:14
theater (4)
4:20;39:16;136:8;160:14
theaters (2)
12:7;155:21
theft (4)
21:8;94:5;109:17;124:8
thefts (1)
20:8
theme (1)
44:4
Thereafter (1)
77:8
Therefore (6)
11:8;39:15;65:3;69:21; 96:9;135:15
thereof (1)
20:18
Third (3)
127:10;145:5;154:3
THOMAS (1)
3:13
Though (1)
34:21
thought (9)
20:4;38:2;42:7;44:8,20; 76:21;81:15;113:9;165:5
thousand (3)
131:5;149:9;158:4
thousands (2)
11:1;117:3
threat (10)
29:1,4,11;60:14;128:2; 131:18;136:9;142:20; 144:18;145:21
threats (3)
28:15;140:6,7
three (14)
7:3;14:5,16;16:6,9;29:9; 43:16;61:11;125:15; 129:20;142:9;146:4,7,12
throughout (1)
165:1
throwing (1)
162:19
Thursday (1)
1:16
Thus (12)
21:2;23:3;61:6;69:20; 80:13;91:5;107:15;122:6; 123:9;129:12;133:20; 159:20
tie (3)
48:12,15,17
tier (1)
28:10
timeline (1)
118:1
times (21)
11:13,14;13:4;16:8; 25:14;26:21;32:20;33:2,3; 34:3;43:1,1,9;46:6;51:9; 90:5,6,13;105:16;106:14; 160:12
titled (1)
105:2
today (2)
125:21;165:18
together (3)
46:21;88:18;137:18
told (7)
33:21;97:4;107:8;120:1; 127:1;131:4;142:10
took (26)
2:5;5:11;14:18;34:16; 39:20;44:19;45:1;57:18; 69:19;77:12;79:20;117:16, 19;119:3,6;122:8,11; 123:17;127:20;128:17; 132:19,19;134:15;162:7; 163:16;167:1
tool (4)
65:11;102:15;145:13; 159:2
tools (2)
60:6;115:18
TOOMAN (1)
3:12
top (9)
31:11;54:11;55:21;66:21; 71:14;91:14;106:7,14; 113:4
topics (2)
37:1;46:1
torture (1)
79:2
total (4)
11:14;106:8,9;126:5
tour (1)
8:14
towards (1)
44:5
town (1)
103:10
track (4)
9:11,12,15;141:9
tracks (1)
47:3
traditionally (2)
52:12;101:6
train (1)
80:19
trained (9)
7:12;10:21;42:8;106:19; 107:2;136:7;150:3;156:9; 165:8
training (15)
18:7,10;37:19;42:11; 44:9;60:19;120:13;136:17; 138:17;141:5;146:17; 147:6;157:10;162:20; 165:11
traitor (2)
166:20,20
transcript (6)
2:2,10,12;36:16;37:11; 45:4
transfer (3)
15:8;117:9;123:18
transferred (1)
15:3
transferring (3)
69:1;123:20;161:16
transgressions (1)
47:7
transition (1)
71:1
translated (1)
2:14
transmission (5)
15:7;17:8,14;90:9;91:12
transmit (3)
90:21;117:12;129:17
transmitted (5)
31:9;42:2;45:20;134:3; 162:17
treat (1)
107:3
treated (2)
31:14;35:20
treatment (1)
44:16
trend (1)
140:12
trends (3)
6:6,14;11:7
tried (1)
58:12
tries (2)
110:21;163:11
trigger-happy (1)
166:13
trip (1)
145:5
Tripp (1)
64:11
troop (3)
9:15;107:20;108:1
troops (1)
107:21
trophies (1)
165:3
trophy (1)
20:10
troubled (2)
20:2;166:16
true (8)
4:13;37:2;75:9;129:11; 141:3;147:5;150:21;152:19
truly (1)
4:16
trust (5)
133:7,18;138:15;164:13; 165:11
trusted (3)
133:3,4;165:9
trusty (1)
53:13
truth (1)
148:12
try (1)
149:20
trying (2)
117:17;148:17
T-SCIF (1)
39:20
TTP (6)
9:19;37:8;107:20;140:4; 155:14;156:6
TTPs (8)
4:21;7:19;24:10,12;26:5; 60:19;123:7;140:17
turn (1)
44:15

turned (3)
53:13;63:20;84:6
turning (1)
84:8
twice (1)
105:16
two (22)
7:1,6;11:3;14:12;45:17;
49:17;50:1;53:13;57:20;
66:12;71:2;107:4;116:9,12;
130:17;138:11,11,17;
151:20;154:4;165:19,19
two-week (1)
91:7
txt (6)
17:13;40:6;74:8;92:11,
13;116:6
type (18)
5:7;8:8;9:4;23:1,4,5;36:8;
65:9;83:6;107:13;116:6;
124:15;130:9;146:19;
156:17;158:1,8;160:2
types (4)
31:2;66:8;116:10;138:6
typical (1)
34:4
typically (1)
120:5
typing (2)
84:3;86:15

U

UBL (3)
153:5,9;156:16
UBL's (2)
153:3;154:12
ultimate (1)
48:15
ultimately (12)
8:16;31:9;34:11;35:4;
38:7;41:4;89:3;92:16;
93:17;110:8;112:21;119:12
unallocated (2)
117:4,15
unauthorized (11)
29:13;31:3;52:14;59:18;
63:21;64:18;99:1;101:14;
124:10;138:14;142:21
uncensorable (1)
144:8
uncertain (1)
107:6
uncertified (1)
2:12
unclassified (5)
44:19,20;117:11;124:9;
162:12
unconventional (1)
18:18
under (8)
14:8;41:5;52:9;58:15;
99:15,17;101:6;114:2
underlying (1)
67:10
undermine (1)
157:16
underscore (3)
14:9,10,10
understands (1)
7:14
understood (8)
83:20;131:4;138:5;139:2;
150:6;154:15;158:11;
166:21
Undeterred (1)
91:2
unedited (1)
2:12
unfettered (1)
165:17
unilaterally (1)
34:17
unique (6)
49:12;61:16;65:16;77:20;
88:12;155:20
unit (20)
5:7;7:2,8;10:18;38:15,17;
64:10;77:11;97:4;107:1;
111:4;112:15;123:5;132:6,
20;133:19;137:19,20;
155:14,16
UNITED (103)
1:2,4;9:6;10:4;18:16;
21:21;22:5,7,15,20;24:9;
26:2;27:7,10;28:3,4;29:2;
30:14;33:7;35:2;36:19;
44:17;46:1;49:2;57:10;
60:7,14,17;61:3;68:5,11,13,
17;69:13;70:6;71:8,12,13,
19,21;75:5,16;76:10,17;
77:21;78:4;94:16,21;95:2,5,
15;96:12;102:9,16;103:14;
105:5;107:10;108:3;119:7;
120:3;122:16;123:7,13;
124:17,19;129:5;130:6;
131:12;132:13;134:10,12,
17,19;135:9,14,21;136:18,
20;137:19;143:3;144:12;
146:10;148:18;150:2,12;
151:4;153:2;154:5,8;
155:19;156:1,7;157:8;
159:7,16;161:6;164:4;
165:7,8,16;166:1,3,18
units (3)
24:12;26:4;123:8
unknown (1)
101:10
unless (2)
107:8;117:15
unlike (3)
97:17;102:1;148:12
unofficial (1)
123:19
unprecedented (1)
161:1
unquestionably (2)
126:7,15
unredacted (2)
93:21;111:15
unsatisfactory (1)
39:11
unsecure (1)
119:12
untracable (1)
144:9
up (14)
12:11;53:11;54:21;63:12;
71:9;79:10;83:8;87:18,19;
102:8;115:5;119:12;131:7;
149:10
uploaded (1)
40:1
uploading (1)
161:19
uploads (1)
66:9
upon (4)
34:16;56:1;120:11;
148:14
upset (2)
113:8,10
urged (1)
127:7
use (37)
4:9;5:13,14,16;6:9;7:13;
8:7,9;10:4;22:8;28:3,16;
35:14,14;44:20;58:2;68:14,
14;99:19,21;100:3;101:16;
109:18;110:10,21;117:7;
136:11;137:4,18;138:19;
139:18;141:10;150:3;
156:5;157:4;159:17;165:9
used (42)
9:8;40:7;43:8;46:12;
47:8;52:2;56:20;57:1,2;
65:16;73:7;76:9;77:21;
80:16;81:4;85:4;87:9,15,
17;88:17,19,21;89:12;
97:18;98:9,16;100:9;
101:13,15;111:20;116:17;
118:12;120:2,2;135:13;
137:16;146:14;156:9;
160:4;163:1,6;165:11
useful (9)
23:5,6;67:9;75:8;80:21;
146:20;155:8;159:10,11
user (58)
47:8;48:7,7,8,8,9,10,12,
15,18,20;49:3;50:2,14,15;
53:4,9,12;54:2,19,20;55:3;
56:8;57:10;58:2,4,9,13;
61:19;62:13;64:10;65:3;
82:5,10,17,18;83:14,18;
86:17;89:14,20;96:21;97:1;
99:9,14,16;106:14;110:17,
19;111:1;112:1,6,7;116:5;
118:7,18;121:9,11
users (5)
12:11;80:6;85:10;110:10;
122:12
user's (4)
52:11;78:12;110:13;
118:19
uses (4)
49:13;98:10;130:3;
141:12
USFI (1)
114:9
using (30)
6:6;14:2;28:15;45:16;
50:14;52:6,19;55:14;57:19,
21;58:11;59:18;60:6;62:12;
68:19;78:21;81:9;82:19;
83:14,19;86:14;87:20;88:5;
89:15,18;96:2;102:14;
109:21;118:15;142:4
utility (4)
16:2;51:15,20;150:6
utilized (1)
138:6
utter (1)
130:12
utterly (1)
39:10

V

VA (1)
1:11
valuable (4)
8:14;70:4;123:4;134:7
valuation (3)
25:1;26:10;70:19
value (28)
6:20;8:6,13,18,20;24:1;
25:7,16;26:15;37:20;49:12;
53:9,10,19;55:6;57:4,13;
58:8;60:14;66:8;121:1;
138:2;140:19;143:9;150:7;
159:13,20;166:21
values (2)
56:3;57:2
VBA (3)
115:9,10,14
verbatim (3)
2:9;36:16;37:12
verify (1)
43:15
version (13)
27:19,21;32:7,8,9;41:19;
44:2;51:1;86:2;91:14;
153:11,18;157:3
via (1)
43:17
Victor (2)
67:8,10
video (66)
34:20;35:1,7,16,20;36:6,
18;37:2,6,14,20;38:2,7,11,
14,16;39:5,14;40:2,11,12,
15,21,21;41:4,13,19;42:12,

17,21;43:10,15,18;44:14, 16,19;45:4,5;103:8,9,9,17, 19;105:1,12,18,20;106:2, 12,15;128:4;129:10;134:3; 152:15;153:15,16,18,21; 154:1,20;155:5;156:19; 157:4,4,8;159:19
videos (1)
105:6
view (11)
14:1;50:17;52:2;78:12; 82:10;83:18,19;86:18;88:5; 157:7;163:4
viewed (5)
20:9;32:4;33:8;142:14; 145:7
viewing (2)
33:10;41:13
views (1)
83:10
violated (4)
57:20;64:19;99:1;118:15
violating (1)
109:20
violation (1)
44:17
violently (1)
163:11
virtual (1)
112:13
Virtually (1)
42:14
visited (2)
104:3;160:8
visiting (1)
15:8
Visual (3)
115:15,15;116:3
visualize (1)
6:3
VOLUME (5)
1:1;17:12;40:5;92:11,13
volumes (4)
74:7;92:11;164:9,9
voluntarily (1)
135:19
voluntary (1)
136:1
von (1)
3:8
VS (1)
1:5
vulnerabilities (1)
34:13
vulnerable (2)
112:8,20

W

wage (2)
69:17;159:6
wait (4)
83:7;86:19;87:19;105:6
wake (1)
149:10
walked (1)
102:8
wantonly (1)
130:6
wants (2)
20:3;163:12
war (8)
18:17;129:7;141:2;157:8; 163:20;165:13,14;166:19
warfare (3)
4:13;141:3,14
warned (2)
30:10;136:11
warning (2)
30:18;78:11
warnings (1)
33:13
Warrant (2)
35:8;121:19
wars (2)
5:1;155:12
wartime (2)
35:18;155:18
watched (1)
45:20
watching (2)
2:6;161:9
way (11)
11:11;52:4,14;53:11; 55:2;57:4,9;83:6;125:6,13; 130:19
ways (4)
49:7;57:20;116:3;166:5
weaknesses (2)
164:16,18
weapon (1)
108:2
weaponry (1)
10:4
weapons (2)
37:9;141:10
Weaver (7)
52:8;98:20;99:2,6,14; 101:1,4
web (39)
32:6;61:21;63:4,13;69:3; 73:3,7;82:6,7,10,13,19; 83:5,8,9,10,19,19;86:14,14, 17,19;87:10,11,12,18,20; 88:5,13;89:15;98:18; 102:14,21;103:21;106:13; 138:8;141:11;157:12; 163:14
website (24)
29:2,20;30:9;32:12,15; 33:9,10;62:2;66:18;68:20; 72:4;82:18;104:10,15; 105:4;142:8,14;143:14,16; 145:15;146:14;160:6,9,19
week (4)
69:16;105:21;122:3; 161:2
weekly (3)
6:13;10:13;140:5
weeks (3)
10:5;33:11;45:17
Weiss (8)
80:1,7,13;82:8,14;83:13; 87:6;89:14
well0intentioned (1)
164:5
well-informed (1)
160:10
well-intentioned (2)
164:7,19
well-known (1)
141:15
weren't (1)
154:1
west (1)
159:7
western (1)
159:6
Wget (67)
48:14;59:18;63:21;64:3, 6,18;65:1,2,2,10,14,17,20; 66:1;68:19;84:7,8,18,20,21; 85:2,5,7,9,13,13,16;86:3,6, 7,8,10;87:10,15,17,20;88:9, 19,19;89:5,12,17,18;91:5; 93:18;96:14,16;97:11,14, 15,17;98:1,6,9,10,12,15,18; 99:17;101:9,13,15,16,18, 20;102:3,19
Wget-H (1)
65:9
What's (5)
37:18;81:15;90:17;115:3; 135:10
whereabouts (1)
9:17
whereas (2)
65:20;89:14
Whereupon (1)
42:3
whistleblower (1)
166:20
White (2)
97:11;161:19
whole (1)
41:19
wholesale (1)
152:6
whose (2)
119:2;162:14
WHYTE (1)
3:7
Wide (1)
163:14
widest (1)
42:16
WikiLeaks (141)
4:11;8:9,10;15:4,9;17:8, 19;18:5,5,6;20:13;21:4,18, 20;28:4,6,21;29:2,4,9,18; 30:1,2,20;31:9;33:15;34:10, 11,13,21;35:4;38:8;40:1,11, 16,19;41:5;49:5;53:14,19; 54:1,8;56:12;58:11;60:1,8; 66:17;67:1;68:2,4;75:12; 76:5;77:1,4,13;90:10; 91:12;92:17;93:6,8,20; 94:13,15;103:7;105:11,16; 106:2;108:18;109:4; 113:17;116:19;117:12; 123:20;126:6,8,16;127:2, 11,15,16,21;128:2,3,5,11, 16,20;129:1,15,18,18; 130:20;134:5,8;135:14,15; 136:3,10,11;138:20;140:20; 141:20;142:8,11,18;144:1, 4,6,8,10,18;145:8,10,14,21; 146:8;147:10,13;148:1,7, 14,21;149:3,5;152:9;153:7, 10,19;154:1;155:2;159:11, 14;160:5,6,11,11,16,19; 161:7,8;164:1
WikiLeaks' (1)
126:19
WikiLeaksorg (2)
28:20;79:9
Wikipedia (1)
144:8
Williamson (6)
109:7;114:12;115:15; 116:2,9,16
win (1)
5:1
Window (2)
85:18;102:2
Windows (12)
49:7,11,16,17,20,21;50:8, 9,12,18;53:2;74:12
Winter (1)
159:4
wiped (3)
15:12;16:11;17:9
wiping (2)
16:7;165:4
within (27)
9:9;10:5;14:4;19:4;21:1; 22:12;23:10;24:5;33:4; 45:7;48:14;53:2;56:11; 76:14;94:17;103:19;104:3; 110:9;115:16,21;119:17; 131:19;132:12;144:12; 156:14;157:11;158:10
without (19)
8:12,19,20;30:3;33:5; 41:13;48:12,17;89:19; 92:19;97:16;120:16; 130:11;131:4;136:15; 139:3;143:5;145:16;146:2
witness (7)
23:16;67:7;70:8;95:6; 101:10;122:18;123:15
witnesses (6)

67:5;107:19;111:14,20; 129:9;134:11
wmv (2) 103:16;105:2
woke (1) 131:7
Woods (2) 61:4,9
word (2) 2:15;120:2
Words (15) 4:10;49:10;82:19;96:3,8; 108:2;133:10;136:13; 139:8;147:8,20,21;151:11; 162:9;166:7
work (15) 12:15;28:16;45:18;58:14; 69:10,20;81:21;122:3; 136:7;140:2;141:6;148:15; 156:4;162:5;165:4
worked (4) 28:14;69:12;82:2;121:8
working (4) 90:8;112:4;113:2,7
works (1) 69:16
worksheet (3) 91:14,18,21
world (23) 19:6;28:6;34:17;35:5; 77:14;81:16;113:16; 127:10;129:14;131:6; 134:6;136:3,14;148:2; 149:9;162:21;163:4,5,14; 164:3,3;166:6;167:2
world's (1) 45:21
worldwide (9) 19:12;84:14,16;140:6; 147:15,16;155:19;156:1,16
worm (1) 9:17
worth (4) 25:11;26:19;81:12;96:10
write (2) 115:10,10
written (4) 14:15,16;41:14;115:1
wrote (1) 18:1
wrought (1) 62:15

X

Xerox (1) 125:17
xlsx (5) 91:15,16;92:3;93:4,12
XXI (1) 1:1
xxx-xx-9504 (1) 1:7

Y

yadda (2) 13:15;14:4
year (2) 38:10;154:14
years (7) 7:3;11:2;46:8;132:14; 138:9;151:20;157:11
York (1) 34:3
young (1) 166:16

Z

zip (7) 74:4,9,11;92:10,14; 93:14;105:2

0

000 (5) 63:4,5,6,13,16
09 (1) 46:5
09:30 (1) 167:5
0930 (1) 126:1

1

1 (31) 12:21;13:6;15:7,9;16:1; 24:13,15,20;27:15,15; 32:10,15,16;33:9;40:6,6; 41:8;45:10,12;47:1;65:7, 12;126:4,10,11,11,12,20; 130:5;142:16;144:4
1:30 (1) 1:16
10 (19) 26:16,20;90:9;103:4,4; 104:2;105:2,7,9,12;106:4,6; 107:9;121:13;123:12; 132:14;138:9;148:5;157:11
10:28 (1) 46:12
100 (4) 19:1;138:8;157:12; 160:12
100,000 (1) 130:16
102 (2) 91:13,19
103 (1) 13:7
104 (5) 92:2,9;134:1,9;155:7
11 (3) 63:17;79:21;105:16
114 (2) 32:20;33:3
12 (4) 46:8;63:15;74:19;76:14
12,000 (1) 121:15
12:55 (1) 74:12
12010 (1) 75:19
122 (2) 113:20;114:11
123 (3) 47:21;53:16;54:12
1233 (1) 122:4
125 (5) 16:3,4;51:14,15,19
126 (2) 15:14,19
127 (4) 40:5;74:8,14;92:13
128 (2) 104:11,17
129 (3) 104:7,7,19
13 (8) 34:8;40:2;60:5;75:19; 76:14,21;81:19;109:12
130 (3) 54:3,7;55:20
138 (1) 130:17
14 (7) 32:10;39:16;72:5,6; 144:5;145:9;161:1
141 (2) 75:17;106:7
144 (3) 11:14;114:18;115:2
145 (1) 115:13
147 (2) 111:7,13
148 (1) 111:14
15 (10) 27:15,17;35:5;39:17; 58:19,21;75:13;81:18; 127:21;143:11
15:55 (2) 53:17,18
152 (1) 13:3
153 (4) 134:21;153:12,12;154:7
154 (4) 72:18,21;73:10,18
157 (3) 64:2;84:19;85:7
159 (3) 89:21;90:3,11
15-minute (1) 125:4
16 (5) 72:5,6;108:8;109:16; 159:3
16:11 (3) 53:17,18;56:17
16:11:26 (1) 56:10
1609 (1) 55:10
169 (5) 78:6,8,14,15;79:12
17 (1) 73:11
17:48:51 (2) 51:10,10
173 (2) 154:13,19
174 (1) 155:3
177 (3) 78:7,8;79:13
178 (2) 78:15,16
179 (2) 16:18,19
18 (2) 28:18;74:19
180 (6) 19:2;72:6;74:18;75:6,12, 13
1807 (1) 72:5
181 (5) 31:15,16,21;74:18;75:6
182 (2) 135:2;153:21
186 (1) 45:8
187 (1) 87:13
188 (2) 86:5,5
189 (1) 65:7
19 (5) 32:20;33:4,9;46:6;142:14
1966 (1) 79:10
1AAB (1) 111:6

2

2 (27) 4:8;22:10,19;25:2;26:7; 27:17;34:20,20;51:9;59:11, 11;64:20;71:3,10;76:15,15; 103:4,5;104:3;108:8;126:5, 11,13;130:5;131:15; 145:12;153:2
20 (2) 40:1;75:13

20,000 (1)
45:20
20,10 (1)
16:8
200 (2)
63:12,13
2004 (2)
11:2;155:18
2005 (1)
69:14
2007 (1)
29:6
2008 (7)
28:18,21;109:2,8;113:17;
138:11;144:10
2009 (17)
11:1,2;32:10,16,20;33:4,
11;38:15;62:1,5;103:7;
126:20;142:14,16;144:4;
145:2;155:18
2010 (91)
13:1,6,10,10,13,13,21;
14:16,17;15:7,9,13;16:1;
17:1,4,5,10,15;18:15;20:20;
32:10,10;35:6;39:1,2,8,17,
18;43:2;45:19;46:5,11,15;
47:4;48:3,5;51:10;56:10;
60:5;62:6,13,19;64:4,7;
72:10,16;73:12,15,21;
74:10;75:18;79:10;81:18;
82:1;85:1,3,3,10,11;90:13;
91:8;92:3,6,10,15;93:7,9,
11;97:10;104:3;105:3,7,9,
11,12;108:20;113:6,7;
121:21;127:21;128:3,5,8,
11,15;143:11;144:5;145:9,
9;159:3,4
2011 (4)
66:17;92:17;128:19;
129:1
2013 (1)
1:16
20-page (1)
111:14
21 (3)
30:15;73:15;128:18
210 (8)
6:12;7:20;80:18;81:5;
98:5;100:2;139:21;147:7
21st (2)
4:13;141:3
22 (21)
32:19;39:1,1,7;47:9;
48:21;54:18;64:6;72:14,16;
73:15,21;74:10,12;76:2;
85:15;89:11;90:14;91:15;
128:11;143:19
22:28 (2)
46:11;56:19
22:28:21 (1)
46:16
2200 (1)
56:18
22211 (1)
1:11
23 (1)
63:15
24 (1)
39:17
25 (9)
1:16;15:21;66:17;128:5,
8;129:1;139:6,8,13
250,000 (4)
77:12;83:16;87:4;91:9
251,000 (2)
84:3;89:3
251,287 (5)
92:18;93:1,6,16,20
251,288 (5)
91:21;93:5,12,15,19
25-2 (5)
52:9;98:21;99:1,15;124:4
26 (1)
20:20
27 (2)
85:3;128:15
28 (3)
90:5,6;128:15
285 (1)
45:7
29 (2)
32:9,16

3

3 (29)
13:10,10;26:6;29:12;
41:16;45:10,13;47:1,20;
59:12;64:20;66:10,11;71:3,
9;76:15;90:13;92:3,6;
95:18;96:6;108:8,9,10,14;
109:14,19;145:20,20
3,300 (1)
130:16
3:22 (1)
62:21
30 (9)
13:20;15:13;17:4;25:7,
13;56:18;74:4;83:1;84:15
30-day (1)
11:6
31 (6)
16:7;17:4,9,14;47:4;
92:17
32 (1)
31:12
330 (1)
104:4
35 (2)
81:5;136:18
351C (1)
55:2
36 (1)
43:1
365 (2)
51:16,19
37 (2)
166:14,15
38 (1)
35:2
380,000 (2)
10:8;26:18
382 (2)
51:17,20
390,000 (1)
128:12

4

4 (15)
4:8;26:11;29:12;62:19;
70:17;92:10,15;98:9;108:9,
15;109:14,19;113:4;
121:19;159:4
4,000 (2)
138:9;157:13
40 (5)
19:14;32:11,19;48:21;
69:16
40-hour (1)
122:3
41 (3)
41:7;164:11,15
417 (2)
46:17,17
417,000 (1)
19:17
42 (3)
4:14;19:8;141:4
425 (2)
72:7,10
43 (1)
145:7
44 (1)
159:5
45 (6)
27:20,21;29:12;30:16;
142:15;159:5
4-582 (1)
64:19
4-5A3 (1)
109:21
46 (4)
21:2;27:21,21;142:16
47 (3)
111:7,9;116:13
470,000 (3)
14:19;17:3,11
48 (5)
16:6;111:7,9,12;116:13

5

5 (18)
4:8;14:15;22:10,19;35:9;
62:3,6,13,18;65:21;66:11,
11;95:17;105:11;123:9;
128:3;163:8,9
5:45 (1)
167:9
504 (1)
106:8
51 (3)
43:1,1;121:15
52 (2)
137:6,11
53,000 (1)
90:12
534 (2)
43:3,4
56,000 (2)
69:20;70:2
5-8-2010 (1)
35:5

6

6 (6)
4:8;46:5;48:2;53:15,17;
95:21
61 (1)
43:9
617 (9)
23:18;27:11;70:8;71:15;
72:2;95:7;96:13;122:18;
123:14
628 (2)
105:14,14
63 (1)
32:14
64 (1)
33:1
640 (2)
105:14,15
641 (1)
121:6
668 (2)
43:3,4

7

7 (21)
4:8;12:21;13:6,13,13;
22:10,19;32:17;63:18;64:4,
7;66:1;70:16;85:1,3;
105:12;108:20;109:8;
161:2;166:14,14
700 (2)
69:18;129:2
700,000 (8)
90:5,6;126:6;130:14;
136:2;163:17;164:1;165:13
72 (4)
11:2,13;137:11,11
74,000 (5)
111:10;119:18;121:5,14;
122:11
740,000 (1)
121:14
75,000 (1)
128:6
78 (2)

16:4,5
7-month (1)
130:15
7-pass (2)
16:6;47:5

8

8 (17)
14:17;46:5,11,15;48:5;
53:17,17;56:10;59:10;62:1,
5;70:21;113:6;161:2,13;
162:13;166:15
80 (3)
55:17;69:9,20
80C1 (1)
56:5
80C1049 (1)
55:2
81 (7)
43:3,6;46:17,18;72:7,11;
105:13
82 (7)
62:9,16,18,20;63:5,15,19
84 (1)
32:1
86 (2)
16:5,5

9

9 (11)
59:8,11;72:10;75:18;
84:16;90:6,6;113:7;123:2;
147:18;148:4
90 (4)
19:1,2;69:9;106:7
90,000 (3)
10:10;25:10,13
900 (2)
96:4,4
95 (3)
66:19,20;162:10